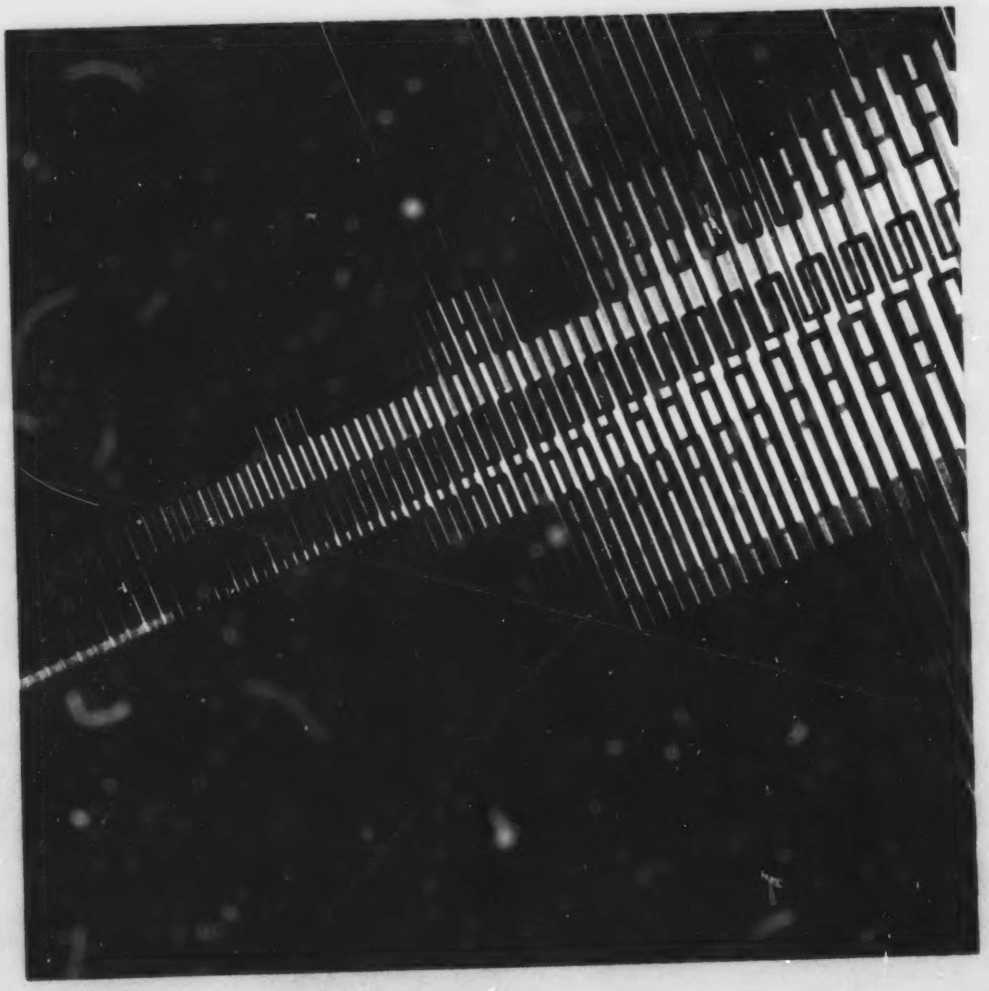
CROSSING THE BORDERS OF PRIVACY

Transborder Flows of Personal Data from Canada



Department of Justice Canada
Ministère de la Justice Canada

92-06448/

CROSSING THE BORDERS OF PRIVACY

Transborder Flows of Personal Data from Canada

by

René Laperrière, LLD (Montréal)
Professor, Department of Legal Studies
Université du Québec à Montréal

René Côté, LLD (Paris X)
Professor, Department of Legal Studies
Université du Québec à Montréal

Georges A. Le Bel, PhD
Legal and Political Sciences (Paris I)
Professor, Department of Legal Studies
Université du Québec à Montréal

Pauline Roy, LLL (Montréal)
BSc Political Science (Ottawa)
Assistant Professor, Law Faculty
Université de Montréal

Karim Benyekhlef, LLM (Montréal)
Assistant Professor, Law Faculty
Université de Montréal

A study undertaken by the Computer Science and Law Research Group, commissioned by the Government of Canada

March 1990

CANADIAN CATALOGUING IN PUBLICATION DATA

Main entry under title:

Crossing the borders of privacy : transborder flows of
personal data from Canada

Issued also in French under title: *Vie privée sans frontières*.
At head of title: Computer Science and Law Research Group.
Includes bibliographical references.
JUS-P-583
ISBN 0-662-18562-5
DSS cat. no. J2-109/1991E

1. Transborder data flow — Canada. 2. Computers — Canada — Access control. 3. Data protection — Canada. 4. Privacy, Right of — Canada. I. Laperrière, René, 1944 - . II. Université du Québec à Montréal. Groupe de recherche en informatique et droit. III. Canada. Dept. of Justice. IV. Title: Transborder flows of personal data from Canada.

QA76.9.T7C75 1991 005.8 C91-098547-2

This report is published by authority of the Minister of Justice
and Attorney General of Canada

by

Communications and Public Affairs
Department of Justice Canada
Ottawa, Ontario
K1A 0H8

(613) 957-4222

Également disponible en français sous le titre
Vie privée sans frontières

Graphic Design: Jacques Charette and Associates Ltd.
Cover illustration: Maurice Macot, Université du Québec à Montréal

©Minister of Supply and Services Canada 1991

Printed in Canada

FOREWORD

The Standing Committee on Justice and the Solicitor General, in its review of the *Access to Information Act* and the *Privacy Act*, advised the government in 1987 to examine the impact of transborder flows of data in the private and public sectors, with a view to protecting the personal information of Canadian residents. The task was given to the Groupe de recherche informatique et droit (computer science and law research group) of the Université du Québec in Montréal.

The Department of Justice expresses its thanks to the authors of this study. Their expertise in matters relating to the protection of personal information, and their knowledge of the legal system, have resulted in a publication that will serve as a valuable reference document for anyone looking into the transborder flows of personal data. The results of other studies by this group on the protection of personal information, and on computers and the law, can be found in the publications *L'identité piratée* and *Une démocratie technologique*.

The special contribution of Louise Potvin, Department of Justice legal counsel and specialist in the protection of privacy, is also acknowledged. As coordinator of the project, Dr. Potvin was a vital link between the research group and the Department, especially during the drafting of the text.

TABLE OF CONTENTS

INTRODUCTION
THE RESEARCH MANDATE 1

1 **The context** 3
2 **Objectives of the study** 5
3 **Methodology** 7

PART ONE
STATEMENT OF THE ISSUE 9

1 **Review of the literature** 11
1.1 Bibliographies 11
1.2 Quantitative studies 12
1.3 Publications on legislative aspects 16
1.4 Consultation with experts 16
2 **Analysis of legislation** 16
2.1 The issue and the analytic categories 17
2.2 The legislative situation 18

PART TWO
CONDUCT OF THE STUDY 23

1 **Preparation of the questionnaire** 25
2 **The population** 26
2.1 Establishing the population 26
2.2 Comparison with populations examined in other studies 30
3 **Questionnaires sent and received** 32
4 **Mail received** 34
5 **Telephone calls received** 38
6 **Rate of response to the survey** 39
6.1 Calculation of the rate of response 39
6.2 Comparison with response rates in the other studies 39
6.3 Explanation of the rate of response 41
7 **Coding and analyzing data and preparing tables** 42
7.1 Coding 42
7.2 Determining the activity and sector of activity 43
7.3 Preparing the statistical tables 45

8 Definition of sectors, groups of sectors and subsectors 45
8.1 The private sector 45
8.2 The public sector........49
9 Rates of response by sector and group........51
9.1 The rate of response overall and by sector 51
9.2 Results for public sector groups 52
9.3 Results for private sector groups........54
10 Rates of response by subsector........56
10.1 Tabulated results 56
10.2 Interpretation of rates of response 61
10.3 Differences between responses received and responses processed........64

PART THREE

CHARACTERISTICS OF RESPONDENTS 67
Explanation of the presentation and interpretation of the results 69
1 The occurrence of transborder flows 73
1.1 Overall results by large sector........73
1.2 Comparison with the results of other studies 74
1.3 Results for public sector groups 75
1.4 Results for private sector groups........77
1.5 Results by public sector subsectors........80
1.6 Results by private sector subsectors........81
1.7 Significant variations among subsectors........85
1.8 Summary and conclusions 86
2 Number of clients........88
2.1 Results overall and for large sectors........88
2.2 Results for public sector groups 91
2.3 Results for private sector groups........93
2.4 Calculating the indices of the significance of the number of clients........96
3 Number of employees 99
3.1 Results overall and for large sectors........99
3.2 Results for public sector groups 101
3.3 Results for private sector groups........104
3.4 Calculation of the indices of significance of the number of employees........106
3.5 Summary and conclusions concerning size of respondents 108
4 Jurisdiction 109
4.1 Results overall and for large sectors........109
4.2 Results for public sector groups 111
4.3 Results for private sector groups........112
4.4 Summary and conclusions 114

PART FOUR
CHARACTERISTICS OF EXPORTS 117

1 **Transfers to intermediaries** 119

2 **Transferees** 122

2.1 Rate of response 122
2.2 Analysis of results overall and by large sector 123
2.3 Results by groups of subsectors 124
2.4 Summary and conclusions 127

3 **Purposes of disclosures** 128

3.1 Rate of response 128
3.2 Analysis of results 129
3.3 Summary and conclusions 136

4 **Volume and frequency** 137

4.1 Categories of persons who are the subjects of disclosures 138
  1. Multiple disclosures 138
  2. Results overall and for large sectors 139
  3. Results for groups of sectors 140
  4. Summary and conclusions 143
4.2 Frequency of disclosure 143
  1. General characteristics 143
  2. Estimate on an annual basis 145
4.3 Volume of transfers 149
  1. Rate of response 149
  2. Transfers of data about clients 151
  3. Transfers of data about employees 159
  4. Transfers of data about "other" persons 164
4.4 Summary and conclusions 165

5 **Nature of the data** 167

5.1 Determination of the nature of the data 167
5.2 Number of responses 168
5.3 The major identifiers 169
5.4 Identification numbers 170
5.5 Other identifiers 172
5.6 Socio-economic status 173
5.7 Health 175
5.8 Physical characteristics 175
5.9 Legal history 176
5.10 Memberships and affiliations 177
5.11 Applications, correspondence and opinions 177
5.12 Summary and conclusions 178

6 **Methods of transfer** 180

6.1 Rate of response 180
6.2 Analysis of results 181
6.3 Summary and conclusions 183

7 Forms of disclosure 184
7.1 Rate of response 184
7.2 Analysis of responses 185
7.3 Results of earlier studies 187
7.4 Summary and conclusions 188
8 Protection and guarantees 188
8.1 Protection 188
8.2 Guarantees provided by transferees 191
8.3 Summary and conclusions 194
9 Very large volumes of exports 196
9.1 Insurers 197
9.2 Other private sector exporters 200
9.3 Public sector exporters 204
9.4 Summary and conclusions 206

PART FIVE
COUNTRIES OF DESTINATION AND LEGAL PROTECTION 209
1 Overall situation 212
1.1 Overall results of the survey 212
1.2 Typology of countries of destination 219
1.3 The European countries 222
    1. International instruments 222
    2. Protection relating to the nature of the data 226
    3. Protection relating to purposes 227
    4. National protection 228
1.4 The United States of America 232
    1. General framework of protection 232
    2. Sources of the protection 233
    3. Legislative protection 237
1.5 Other countries 241
2 Countries of destination reported by public sector respondents 243
2.1 Results of the survey 243
2.2 Legal protection 246
3 Countries of destination reported by private sector respondents 253
3.1 Results of the survey 253
3.2 Legal protection in the private sector 256
4 Analysis of results by public sector group 261
4.1 Education 261
4.2 Health and social services 262
4.3 Government 264

5 Analysis of results by private sector group 266
5.1 Associations 267
5.2 Insurance 268
5.3 Business and industry 272
5.4 Communications 273
5.5 Financial services 274
5.6 Transportation and tourism 276
5.7 Computer services 277
5.8 Professional services 278
5.9 Miscellaneous services 279
5.10 Residual contextual law 280
6 Summary and conclusions 281

SUMMARY AND GENERAL CONCLUSIONS 283
1 Originality and limits of the study 285
2 Summary of conclusions from the questions examined 289
3 Summary of conclusions by groups of sectors 294
4 Conclusions from the study and significance of conclusions 308
5 Assessment of the research experience and acknowledgments 310

APPENDIXES 313
1 Questionnaire 315
2 Letter of introduction 321
3 Letter from the Data Protection Registrar of the United Kingdom 322
4 Letter from the Bundesbeaufragte für den Datenschutz of the Federal Republic of Germany 323
5 Map of occurrences of transfers per country or continent 324
6 Map of relative occurrences of transfers to the United States ... 325

INTRODUCTION
THE RESEARCH MANDATE

The Computer Science and Law Research Group (GRID) was commissioned by the Government of Canada to conduct a study of transborder flows of personal data about Canadians[1], either through computer transmission or by other means. The parameters were set out in the Statement of Work contained in a request for proposal issued by the Department of Supply and Services July 21, 1989, entitled: *Study of transborder data flows of personal information on any identifiable individual living in Canada, transmitted by computer or any other mode of transmission.*

In response to that request, GRID submitted a study proposal on August 28, 1989, including a technical proposal. When this proposal was accepted, agreements were concluded with representatives of the Government of Canada on the objective of the work and how it was to be carried out. These agreements were set out in a letter sent by GRID on September 19, 1989, to the Science Directorate of the Department of Supply and Services.

1 The context

In a 1987 document entitled *Access and Privacy: The Steps Ahead*, the Government of Canada undertook to implement one of the recommendations of the House of Commons Standing Committee on Justice and the Solicitor General, entitled *Open and Shut: enhancing the right to know and the right to privacy.*

Since this Committee set out the framework for the research mandate given to us by the Government of Canada, it is important that we refer to the relevant aspects of these two documents. The Committee's analysis and recommendations may be found at pages 80 and 81 of its report. The Committee noted that Canadians were especially sensitive to the question of international transfers of personal data by governments and the private sector, using various modes of communication, including transfer by computer and satellite, and concerned that once personal data left Canada they were beyond the control of Canadian law. The report stated that the privacy aspects of these transborder flows of information, unlike economic and trade aspects of this phenomenon, had not received adequate government attention.

The Committee raised a number of questions. Are there provisions in other countries to protect personal data transferred and recorded there? Do such transfers rarely occur from Canada, as the Royal Bank of Canada stated before the Committee? How do we reconcile this assessment with the fact that European countries, with a longer tradition of data protection than Canada, have discovered significant transfers in such fields as labour, multinational business (the transfer of personnel data) and medical research?

---

[1] In this study, such persons are identifiable individuals living in Canada.

The sectors, organizations and activities identified by the Committee for investigation were banking, credit information systems, credit card services, health care information, labour unions, personnel and payroll records, airline travel reservations and general government activities. These were identified because international data transfers in these areas are subject to controls under European data protection legislation.

The Committee referred to medical information routinely transmitted by Canadian life insurance companies to the Medical Information Bureau (MIB) in Boston, Mass., which maintains 620,000 files on the health experience of Canadians. It questioned what fair information practices were in place at this foreign organization, given that it was beyond the reach of Canadian law.

The Committee agreed that Canada must be concerned about this issue and bring together the necessary resources to carry out a special study of the issue by those federal institutions that already have significant responsibilities within the government for the privacy aspects, and other important aspects, of transborder data flows, such as the Department of External Affairs and the Department of Justice. Such a study should bring together representatives of various federal government agencies (Department of Communications, Privacy Commissioner, Canadian Radio-Television and Telecommunications Commission, Science Council of Canada), as well as provincial agencies, specifically to examine the implications for Canada of the coming into force on October 1, 1985, of the Council of Europe's *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. This statement is quickly becoming the major international statement on data protection.

In support of its assessment of the issue, the Committee cited the Annual Report of the Privacy Commissioner (1985-1986), the report of the Ontario Commission of Inquiry into the Confidentiality of Health Information (the Krever Report), GRID's 1986 report entitled *L'identité piratée*, and the 1981 Report of the Council of Europe on the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*.

The Committee's recommendation 7.12 reads as follows:

The Committee recommends that the Government conduct a review and study of the implications of transborder data flows by the public and private sectors for the personal privacy of residents of this country. Such a study should be tabled in Parliament within one year of the tabling of the Committee's Report.

Later in 1987, the Government of Canada tabled *Access and Privacy: The Steps Ahead*, its reply to the report of the Committee. In it, the government considered the issue of privacy protection in Canada and abroad in a discussion that appears at pages 12 and 13 of its reply. It reiterates its commitment to the protection of privacy and individual liberties, as confirmed by its adherence to the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, and expressed in the enactment of legislation (citing the *Privacy Act*) and through the encouragement and support of self-regulation and the establishment of a task force to promote the protection afforded by the Guidelines throughout the public and private sector. The statement of government policy continues:

> *Technology makes it possible to move information across international boundaries with ease. This transborder flow of data could have implications for the privacy of Canadians. The government agrees with the Committee that this matter requires study and has already begun to explore the means by which to determine whether such a problem exists, and if this is found to be the case, the government will move to address it.*

2 Objectives of the study

The primary objective of this study was described generally in the request by the government: it was to explore the extent to which information of a personal nature about Canadians was being transmitted beyond Canadian borders either by computer or other means.

We took this statement to mean that ours was to be an exploratory study consisting essentially of collecting facts on the current situation relating to flows of personal data to points outside Canada, and excluding flows of information that were non-nominative (statistical profiles, for example).

We were also required to study foreign legislation applying to such transborder flows to assess how well protected are exported Canadian data, including the rights of Canadians with respect to data concerning them. It was agreed, as a secondary issue, that we would explore contractual and self-regulatory protection accorded to this information, looking particularly at measures for the protection of confidentiality, codes of ethics and the application of the *lex fori* (to the settlement of disputes).

The Department's request listed five specific study objectives. The first was to determine more precisely the nature of the data transmitted. It requested that all the categories of data set out in section 3 of the *Privacy Act*[2] be considered. By agreement, a number of specific factors were added, relating particularly to a number of common identifiers, as well as language, citizenship, membership in various groups, economic status, credit ratings, opinions and criminal records.

---

[2] RSC, 1985, c P-21

The second objective of the study was to identify the types and characteristics of exporters who transfer personal data to points outside Canada. We agreed to identify the federal or provincial jurisdictions concerned with the activities of exporters of information, as well as the sectors of activity to which these exporters belong. Reiterating the concerns expressed by the Committee, the government statement mentioned a number of areas to be studied: banking transactions (banks and financial institutions), financial information systems (credit bureau networks), credit card services (issuing companies), health care (health care institutions), personnel and payroll records (all sectors), airline reservations (air transport), and information transferred by the government (departments and public organizations) and unions (associations sector). We further proposed to maintain the distinction between the public and private sectors, and to examine several other areas that may be involved in exporting data on Canadians: educational institutions, municipalities, insurers, transporters other than airlines, large hotel chains, and the retail/wholesale, nonprofit association, media and real estate sectors.

The third objective was to determine the destination of the information transferred beyond our borders. Essentially, this involved identifying the countries of destination for the export of data about Canadians and an assessment of the protection accorded to such data. We systematically reviewed the protective legislative provisions in force in the importing countries.

The fourth objective, related to the third, was to determine who receives and retains this information abroad and how it is utilized. Here, we suggested that we verify whether these were internal flows within the exporting multinational firms. Utilization of the information involves the concepts of purpose (for example, providing a service to customers or trading in information) and use (for example, updating or developing statistical profiles).

The fifth objective was to measure the volume and frequency of such transfers. We indicated that we would probably obtain approximations from our respondents in this respect. We also suggested that we attempt to verify how personal information was exported, in terms of means (size of records transferred) and form (telephone, hard copy, magnetic, telecommunication). We further proposed that we inquire into contractual guarantees sought by data exporters, to complete the picture of the protection accorded to data transferred abroad.

3 Methodology

It was agreed that the study would comprise three operations. Firstly, the compilation of relevant statutes and a survey of the literature would be updated. This would facilitate compiling relevant legislation and help locate other empirical studies that might have been carried out on this subject abroad and in international organizations. It would also refine our conceptual tools so that both our questions and the analyses that we might derive from the data collected would be as accurate as possible.

The second operation would consist primarily of a field investigation which, given the very short deadlines imposed by the government, could be conducted only through a postal questionnaire, accompanied by a letter of introduction and followed by two reminders. The mandate also included administering a pre-test, assessing the likely incidence of refusals to respond, and proposing ways in which such refusals could be minimized. For this purpose, it was agreed that we would set out in our letter of introduction that we were commissioned by the Government of Canada to conduct research on the terms described above.

The process that we proposed for conducting the survey was agreed to by the government. It consisted essentially of selecting a population of about 5,000 of the largest public organizations and private firms in Canada, specifically targeting the sectors of activity where it appeared to be most likely that personal information about Canadians would be exported. We then sent them a fairly detailed, closed and codable questionnaire, asking them, not for their opinions, but rather for basic organizational characteristics, types of correspondents and practices (volume and frequency of transfers, countries to which data are transferred, nature of information, anticipated uses, methods and guarantees).

Finally, the mandate included analyzing the data collected, employing the methodology in current use in the specialties in question: preparing and interpreting frequency tables and cross-tabulations by sector of activity; preparing summary tables and comparing results; analyzing the legislation and reviewing the literature; assessing the scope of the phenomenon and the applicable legislative and contractual protection; and stating these analyses in terms of the initial hypothesis in order to verify or modify it on the basis of the results of the study. We paid particular attention to the need, in this final step, to reconcile the observations from the empirical study with the legal principles, to present a conceptual overview of the results of our work as a whole so as to facilitate subsequent examination by legal category.

To carry out this mandate, we propose in this report to present a brief statement of the issue (Part 1), followed by four broad analytical parts dealing with, respectively, the conduct of the study (Part 2), the characteristics of the respondents (Part 3), the characteristics of personal data exports (Part 4), and the countries to which data are transferred (Part 5). This last topic in itself necessitated relatively extensive consideration and became a subject of discussion separate from the other results of the study. These analyses include summaries and provisional conclusions and are followed by a general conclusion setting out summaries by issue and sector, and final considerations, in addition to the technical appendixes.

PART 1
STATEMENT OF THE ISSUE

As we have seen, our mandate was essentially to explore the extent of the transborder flow of personal information about Canadians. To define our objective and our field, and to interpret our results, it was essential to prepare an inventory of the studies and analyses pertaining to our subject. From these, we could prepare a statement of the issue.

To clarify and supplement the survey designed to collect quantitative data by questionnaire, we therefore undertook research to locate similar empirical and analytical studies that could guide us in drawing up the questionnaire and in analyzing its results. Moreover, under our mandate, we were to analyze the legal protection of personal information outside Canada by collecting as much information as possible on foreign privacy legislation. To attain these various objectives, we undertook a review of the literature and of the legislation.

1 Review of the literature

For our review of the literature, we first consulted a number of bibliographies GRID had on hand. We then queried data banks using the DIALOG system to identify texts and articles that might contain material relevant to our research.

1.1 Bibliographies

We consulted the following bibliographies:

BENYEKHLEF, K, *Bibliographie de la doctrine sur les flux transfrontières de données*, 1989, 58 p.

GRID DOCUMENTATION CENTRE, *Aspects relatifs aux flux transfrontières de données; documents en possession des bibliothèques de l'Université du Québec (Badaduq) et du Centre de documentation du GRID*, September 1989, 35 p.

COTÉ, René and JOLIVET, Christian, *Bibliographie sur les services informatiques*, August 1989, 55 p.

COMPUTER SCIENCE AND LAW RESEARCH GROUP (GRID), *Droit, Informatique et vie privée; Bibliographie sélective, canadienne et internationale*, SOQUIJ, 1986, 143 p.

We also queried five data banks "direct" using the descriptors "electronic data processing, personal data, computer network / privacy, confidentiality? / law, legal, legislation"; "data protection / computer?, informatic?". The data banks consulted were: *Books in print*; *British books in print*; *Library of Congress Marc*; *Government Printing Office Reference File*; *Dissertation Abstracts on Line*.

This last bibliographic work (147 pages) was particularly useful because it allowed us to identify several quantitative studies that would assist us in interpreting the results of our survey. We were also able to identify publications dealing with the legal rules applicable to transborder data flows in countries for which it is difficult to obtain information. In the case of the United States, GRID had done a summary study of the legislation in earlier studies. However, given the nature of the protection of personal data in that country, and the decentralized and scattered nature of such protective measures, we also referred to several works to help us report on the protection of personal information there.

1.2 *Quantitative studies*

INTERGOVERNMENTAL BUREAU FOR INFORMATICS, *Enquête de l'IBI sur les pratiques nationales et les pratiques des sociétés concernant les flux transfrontières de données*, November 1983, Rome, 119 p.

EDI RESEARCH INC, *Respondent Report for The State of Canadian EDI: 1988, 1988*, Oak Park, Ill., 25 p.

COMPUTER SCIENCE AND LAW RESEARCH GROUP (GRID), *L'identité piratée*, 1986, Montreal, Société québécoise d'information juridique (SOQUIJ), 363 p.

COMPUTER SCIENCE AND LAW RESEARCH GROUP (GRID), *Quelques données empiriques sur les flux transfrontières de données personnelles en provenance et à destination du Canada*, June 1989, Montreal, 9 p.

KANE, Michael James, *A Study of the Impact of Transborder Data Flow Regulation on Large United States-Based Corporations Using an Extended Information Systems Interface Model*, 1986, Doctoral thesis at the University of South Carolina, Columbia, S.C., 168 p.

ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, *The Internationalisation of software and computer services*, 1989, Paris, 195 p.

SAMBHARYA, Rakeshkumar Bishanlal, *The Impact of Transborder Data Flows on the Strategy and Operations of US Based Multinational Corporations*, 1985, Doctoral thesis at Temple University, Philadelphia, PA., 183 p.

We will set out here the objectives and principal findings of these studies and provide comparisons, as required, to analyze our own data (notably with respect to the population studied, the response rate, the existence of transborder flows of personal data and the form of transfer).

1. Let us start with the earlier studies done by GRID on the protection of personal information. Research had been done in 1985 on private firms doing business in Quebec with the aim of setting out the situation relating to personal information in the Quebec private sector,

which is not covered by specific privacy legislation. This work was supplemented by a comparative study of international documents and national legislation, particularly in Europe and the United States. The principal findings of this study related to the sizable personal information data bases in the private sector, in terms of data gathering and distribution. It demonstrated the inadequacy of Quebec and Canadian law in remedying the problems created by this phenomenon. This research is relevant to our present study insofar as it deals with personal information, concerns Canadian firms and examines international and foreign legal protection.

2. The objectives of GRID's research on personal information disclosures in 1988 were: to obtain information on exchanges and transfers of data in Canada, particularly those by computer matching and the use of universal identifiers, and on the social, political and legal impact of these transfers, in a broad theoretical framework that took into account the reality of technological and institutional change. Some of the analyses and data that came out of this study are still being examined. During the work, a question was posed in both the questionnaire and in interviews as to the occurrence and destination of transborder data flows, including interprovincial and international flows.

   Overall, the study showed that the use of computer matching is relatively limited, largely because it is complex and poorly suited to new technology (micro-computers, networking, etc.). It is used in the public sector to detect fraud and in the private sector for marketing and statistical analysis purposes. Except in very specific sectors (income tax and social programs regarding the Social Insurance Number; health and social services with reference to the medical insurance number), "quasi-universal" identifiers are not used systematically in exchanging data. A relatively high proportion of exchanges of personal information is used to establish quotas and develop profiles, and for decision-making and marketing. Controls on such exchanges are weaker in the private sector than in the public sector, reflecting differences in the law. There is more concern about confidentiality of data than about quality or usefulness. The need for appropriate public control on these activities is therefore still an open question.

   More particularly, the survey showed that there were more international transborder flows of data in the private sector (26% of respondents) than in the public sector (12% of respondents), where interprovincial flows dominated. A little more than half of these international flows (54%) occur internally within firms. The greatest number of exchanges occurred with the United States (27 out of 33 data exporters, or 82%), followed at a distance by Great Britain (nine respondents, or 27%), the rest of Europe (15 respondents, or 45%) and the rest of the world (20 respondents, or 60%). This study produced an analysis of these flows by sector of activity, as well as data on the size of exporters' data bases, with which we will deal later. We would note at this point that the findings of that study tend generally to validate the findings from the survey we are now examining.

3. Apart from these GRID studies, the research closest to this study, in both subject and scope, is the 1983 study done by the Intergovernmental Bureau for Informatics. This study dealt with transborder flows of data (not just of personal data) to determine government policies and the practices and opinions of governments and large multinational corporations, or corporations with international client bases, throughout the five continents. A survey was sent to more than 5,000 corporations or public agencies. In addition to the primary activity engaged in by the organizations and the countries where they operated, the survey obtained a description of international data transfer practices and, particularly, the destination, methods of disclosure, uses and purposes of the data. The Bureau wanted to gather information on the importance and benefits of such disclosures to the respondents as well as the regulation to which the disclosures were subject and the international dimension of certain issues.

   Results were obtained for 80% of the corporations and public agencies in Third World countries. Fewer than 20% of these engaged in transborder data flows of any sort. Almost all of those who did used the telephone or telex for these disclosures; only 29% used computers, and only 25% processed or recorded data abroad. The problems of privacy protection and national sovereignty were of concern to 60% of the respondents. Cost reduction made possible by foreign processing and free circulation of their data and free circulation of data were of concern to only 45% and 39% of the respondents, respectively. In general, respondents did not intend to adopt policies for exporting their data. There was a high degree of indecision arising from the lack of research on the subject and the absence of technical infrastructures. These results must be viewed with caution and seen in the context of the composition of the sample and the origin of the respondents. It should also be noted that the study was seven years old.

4. We also analyzed the results of two studies by American academics for doctoral theses, involving much smaller samples of large American corporations. The studies done by Sambharya (1985) and Kane (1986) deal with transborder flows of data (not necessarily personal). They obtained opinions and perceptions on the effect of restrictions on these flows (Sambharya) and the impact of regulation (Kane). Both theses start from the idea, fairly widespread in the American literature, that statutes and regulations, particularly those in Europe, constitute nontariff barriers to the free flow of data. The studies sought to confirm this hypothesis among what were presumed to be the principal actors. However, they did not succeed in

showing that this point of view prevailed among their respondents. For Sambharya's study, economic restrictions, not regulatory restrictions, were most important (for example, protectionist measures for the benefit of national industry). Fully 69% of Kane's respondents believed that regulation of transborder data flows did not cause serious problems. They did fear, however, that regulation would become a problem in future. Their position is weakened by the fact that only 53% of the respondents stated that they had studied the problem and only 20% had taken action as a result. These two studies permit us to compare the composition of the samples and the response rates. However, they were intended to establish opinions, not facts, and therefore cannot be of help in interpreting our results.

5. The OECD (1989) and EDI Research Inc (1988) studies are also opinion surveys, which used somewhat imprecise methodology (which is not therefore readily comparable to ours). Their objectives were only somewhat tenuously related to ours. The OECD study was related primarily to the size of the market in computer software and computer services industries, the level of internationalization in these industries and the barriers to internationalization. Only incidentally did it seek to determine the opinion of the respondents on the influence of personal data protection legislation. Only 18% of the 155 responding firms believed that personal data protection legislation posed a potential problem for their activities in other OECD member countries. Only 15% thought that such problems could arise with their activities in non-OECD member countries. The OECD experts concluded that restrictions imposed by data protection legislation created few problems for the internationalization of software and computer services.

   The study by EDI Research Inc was designed to measure interest in the electronic form of standardized data transmission between firms, to assess the market for such exchanges and to determine the perception of barriers to the implementation of such exchanges. Concern for the particular sensitivity of personal data that might be sent in such communications was absent from this study. Ultimately, it provides us only with information about the forms of communication currently used for data exchanges. Some 75% of transactions are on paper, 16% are oral (telephone or interpersonal contact), nearly 8% by non-preformatted electronic transfer and nearly 2% by preformatted electronic transfer (electronic data interchange: EDI).

1.3 Publications on legislative aspects

We consulted the following texts and will review the various elements of the legislative analysis later in our study.

CCH, *Guide to Computer Law.* Vols I and II.

OECD, *National reports on transborder data flows.*

OECD, *Situation actuelle et tendances de la protection de la vie privé dans la zone de l'OCDE.*

SMITH, R. E., *Compilation of State and Federal Privacy Law.* Washington, D.C., 101 p.

(PERIODICAL), *Transnational Data and Communications Report.*

We also made extensive use of GRID's legislative data bank (created in 1985 and updated in 1987) on privacy protection legislation. Finally, we located a study of Soviet law that we would have liked to analyze: KUMANIN, E. V., *Sotasialno-pravovye aspekty avatomatizatsii upravleniia*, 1986, Moscow, 108 p (descriptors: Computers; Law and Legislation; Soviet Union, Data Protection; Soviet Union); however, we could not do so because of our lack of knowledge of the Russian language.

1.4 Consultation with experts

Along another line, the presence in Montreal last November of two eminent European specialists in privacy protection, Yves Poullet and Herbert Burkert, permitted us to inquire into the status of work on transborder flows in Europe. We also benefited from work being done by the OECD (Dimitri Ypsilanti) and by the International Chamber of Commerce (Martine Briat) in this area. We must observe that the issue of privacy protection seems to have a less important place in the work of these two organizations than it did in the early 1980s.

2 Analysis of legislation

The second heading of the documentary analysis deals with the existence and scope of protection offered in foreign jurisdictions to personal information concerning Canadians or to information originating in Canada. Assuming that the protection offered by Canadian legislation was known, we examined the degree of protection offered by foreign jurisdictions to data concerning foreigners, considering that certain elements of equivalency are always present in international discussions.

To do this, we established a data bank covering the protection of personal information offered by foreign jurisdictions. That seemed to us to be the best way of structuring the existing data and legislation in a form that would be convenient for this project as well as providing a framework that we could flesh out by obtaining the missing information.

2.1 *The issue and the analytic categories*

We therefore formulated the issue in the following terms: Are nominative data originating in Canada protected? If so, in what countries? Specifically, we must ask the following two questions in respect of each foreign jurisdiction: Are there particular legislative provisions concerning transborder data flows? If so, do these provisions apply to data concerning foreigners and particularly Canadians?

When we asked these questions, we found that Canadian legal categories are not necessarily the categories used in the receiving countries. Moreover, protection varies widely, not only in nature and scope but also with respect to the legal techniques used to guarantee protection. Depending on the country, the protection accorded to personal data may flow from the Constitution, from general legislation, from specific legislation or from case law. These diverse provisions may cover and protect only citizens of the country offering the protection, only natural persons and not corporations, or only residents of the country in question.

For this analysis to be exhaustive we would have to examine every jurisdiction to determine whether personal data are protected. If there is a particular statute, we would have to determine whether it covered personal data concerning foreigners and nonresidents and whether the private international law of each country referred these matters to local law or to specific legislation. Finally, we would have to determine the tests used for attachment in each country. Clearly, these tasks could not be accomplished within the ambit of this study.

For this reason, we phrased the question concerning the country of destination of transborder flows leaving Canada as clearly and exhaustively as possible. We asked that our respondents specify at least the three countries to which they transfer the most data. The responses allowed us to concentrate on the countries with which we, as Canadians, have the greatest volume of personal data flows. We then had to examine the possibility of coupling our analysis of certain purposes, by specific categories of respondents, with the responses concerning destination. That permitted us to specify the legislation and jurisdictions that should be analyzed more specifically in terms of the protection accorded to personal information on foreign subjects.

It must be remembered, however, that apart from the European countries for which we have complete information and the United States (which already presents problems of delicate distinction in terms of the diversity of state jurisdictions), the fragmentary information collected cannot be considered to be definitive and complete. We shall therefore have to be satisfied with noting whether there is legislation in a particular jurisdiction, without voicing an opinion as to the degree of coverage offered by this legislation to data concerning Canadians. Such an opinion is not a fact, but a three-pronged legal opinion dealing with whether such protection exists, whether it extends to foreigners and whether foreigners are subject to such national legislation.

We have a particular jurisdictional problem with federal states, which may be complicated by a private international law problem: in the protection of personal information, who has jurisdiction over information on foreign residents?

Moreover, we found that "second generation" privacy protection legislation tends to consist of provisions divided by sector of activity and to apply specifically to those sectors. It was thus useful to have quantitative data to determine the degree of protection offered by foreign jurisdictions to personal data concerning Canadians. Such quantitative data allowed us to concentrate on the protection offered by the jurisdictions with which Canadians have significant exchanges.

2.2 *The legislative situation*

We have, however, collected data that permitted us to answer these questions as our study progressed. In order systematically to record the information collected, we established a data bank. For this purpose, we separated the data into three broad categories: coverage accorded to Canadian data by legislation (a) in the United States; (b) in European countries; and (c) in all other countries.

These broad categories were established on the basis of the type of legislation that has developed in these three groups. The first (Europe) is characterized by legislation of general application, governing both the public and private sectors. The second (North America) is characterized by legislation of general application governing only the public sector (as is the case, as well, in Australia and Japan), supplemented by sectoral legislation in both the public and private sectors. In the third group, most of the countries have no specific legislation and in some cases may rely on very general common law principles to provide a degree of protection to personal data. Our classification therefore makes it possible to give an overview of the legislative situation in the protection of data in countries to which personal data are exported from Canada.

2.2.1 *The United States*

The largest share of transborder flows of personal data from Canada is destined for the United States. For the United States, we already had a substantial portion of the relevant legislation. The work consisted of classifying and entering into the data bank several thousand pieces of legislation in 21 categories and 53 jurisdictions (federal, 50 states, D.C., territories).

Using the sectoral approach explained above, we grouped the personal data protection statutes by state, using the following classification based on the compilation carried out by R.E. Smith (op. cit.): 1: Arrest records; 2: Banking records; 3: TV cable; 4: Computer crime; 5: Credit information; 6: Criminal justice information systems; 7: Government data bases; 8: Employment records; 9: Insurance; 10: Lists of material sent through the post; 11: Medical records; 12: Miscellaneous; 13: Use of lie detectors in employment; 14: Privacy protection statutes and state constitutions[1]; 15: Privileges; 16: School records; 17: Social security numbers; 18: Tax records; 19: Telephone solicitations; 20: Pre-employment testing; 21: Wiretapping.

However, these categories do not address at this point the thousand-odd legal opinions that would have to be given to answer the question: Does a provision in a specific statute in state "Y" apply to all personal information found "under the jurisdiction of that state"? Or the question: Does state legislation cover only information concerning residents of that state, or citizens of the United States, or foreigners? U.S. constitutional law problems are of some significance in this. In the United States, inter-state commerce is under federal jurisdiction. However, the category "protection of personal information" is not totally covered by the category "commerce" and several aspects of the protection of personal information fall outside that category. Nevertheless, a validly adopted federal statute takes precedence over state legislation on the same subject, to the extent of any conflict between them. There is, however, nothing to prevent states from adopting consistent legislation that does not conflict with the provisions of the federal statute on the same subject, subject to exclusive federal jurisdiction.

2.2.2 *Western European countries*

For the (Western) European countries, we assembled the existing legislation that we had already analyzed in *l'Identité piratée*[2], and we updated and classified this legislation on the basis of the same question: the existence, nature and scope of the protection offered in these jurisdictions to personal data coming from Canada and relating to identifiable individuals living in Canada.

We decided to limit our study at first to those countries that have enacted legislation respecting protection of personal data. We therefore sent a letter (October 24, 1989) to the privacy commissioners (or their operational equivalent) in several countries, including some not located in Western Europe. A reminder letter was sent on December 8, 1989. We believed it advisable to send these letters to the privacy commissioners in the countries in question because these authorities would be best placed to provide information about the specific scope of application of the statutes they were responsible for applying.

---

[1] States which did *not* have such protection in 1988 were: Alabama, Arkansas, Colorado, Connecticut, District of Columbia, Idaho, Indiana, Iowa, Kansas, Maryland, Michigan, Minnesota, Mississippi, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, North Dakota, Ohio, Oregon, South Carolina, Texas, Vermont, West Virginia, Wyoming.

[2] Op. cit., p 18

We asked a very precise question of our correspondents: Does your legislation cover data stored in your territory concerning foreigners? We limited ourselves to this question because we were able, simply by examining the legislation, to determine the provisions that affect transborder flows of personal data and correspond to the general principles in the OECD Guidelines.

We found from preliminary examination of a number of European statutes that their application provisions were laconic: "This statute applies to persons." Does the word "person" cover, in addition to nationals of the country, foreigners who do not have resident status? It therefore appeared that we needed the assistance of the commissioners.

Countries contacted were Austria, Belgium, Denmark, Federal Republic of Germany, Finland, France, Great Britain, Grand Duchy of Luxembourg, Hungary, Jersey, Isle of Man, Iceland, Ireland, Israel, Netherlands, Norway and Sweden.

The replies received from the following countries clearly answered our question concerning the status of foreigners: Austria, Denmark, Federal Republic of Germany, Great Britain, Grand Duchy of Luxembourg, Iceland, Ireland, Netherlands and Norway. The legislation in these countries covered personal data relating to foreigners.

With respect to the others, either we did not receive a reply or the correspondence failed to respond precisely to the question asked. In any case, we had in our possession legislation relating to privacy protection from the following countries: Austria, Belgium, Denmark, Federal Republic of Germany, Finland, France, Great Britain, Grand Duchy of Luxembourg, Hungary, Jersey, Isle of Man, Iceland, Ireland, Israel, Netherlands, Norway and Sweden.

On this point, we followed with interest the work of the advisory committee of the Council of Europe on the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, relating to the concept of "equivalent protection", to which we will return in Part 5.

2.2.3 *Other countries*

With respect to the other countries, we sent a letter to all the embassies accredited to Canada, asking that they provide us with information on their legislation and whether there was legislation protecting any information relating to Canadians that might come to them as a result of transborder data flows. Nearly 150 letters in French or English were sent out on October 6, 1989. We received replies from representatives of the following 29 countries: Benin, Bolivia, Botswana, Brunei, Burma (Union of Myanmar), Cameroon, Chile, Colombia, Costa Rica, Fiji, Gabon, Guatemala, Honduras, Hungary, Iceland, Kuwait, Mali, Morocco, New Zealand, Nigeria, Senegal, Seychelles, South Africa, Switzerland, Trinidad and Tobago, Turkey, U.S.S.R., Vatican, and Zimbabwe.

Some of these countries sent us the relevant documents or advised us there were no such documents or legislation in their jurisdictions: Brunei, Costa Rica, Guatemala, Islamic Republic of Iran, Iceland, Mauritius, Morocco, Papua - New Guinea, Switzerland, Trinidad and Tobago, Turkey, and Zaire. We already had information on Brazil and Poland.

Others promised to send us the relevant documents or suggested that we contact the appropriate specialized offices in their countries. We sent letters in French, English or Spanish, as appropriate, to the following countries: Benin, Cameroon, Colombia, Costa Rica, Gabon, Mali, New Zealand, Nigeria, Senegal, Seychelles, and South Africa.

In Part 5, where we deal with the results of the survey by country of destination for personal information concerning Canadians, we will provide a detailed statement of the legislative protection that applies to such data. We will analyze, in turn, general legislation, legislation that applies exclusively to the public sector (or to certain subsectors thereof) and legislation that applies to various subsectors of the private sector.

PART TWO
CONDUCT OF THE STUDY

We will now describe the main stages in the conduct of our study, in order to interpret the results of the questionnaire survey and the survey of the literature. We will examine, in order, the preliminary work (preparation of the questionnaire and establishing the population), the administration of the survey (sending it out, receiving responses, coding and analyzing the data) and conclude with our calculation of the rate of response to the survey.

1 Preparation of the questionnaire

We have attached the text of the questionnaire as an appendix. The first question asks the respondents to list their characteristics: their field of activity, the number of clients or employees they have and the jurisdiction under which their main activities take place. We did not ask our respondents to indicate their provincial origin because such information would have been difficult to interpret, given the complexity of Canadian organizational and communications networks. A firm with its head office in Quebec, for example, could send out data from offices in other provinces.

The second question, dealing with the data exported, determines whether the firm or organization engages in transborder flows itself or does so through another agency. The third question examines the volume and frequency of such flows. The fourth question deals with the types of firms or institutions to which the information is transferred. The fifth question identifies the countries of destination, separating them into groups by geographic zone and asking that the main country of destination be identified. The sixth question addresses the nature of the information transferred and provides a list of some 40 possible answers. The seventh question identifies the main purposes for which data is transferred. The eighth question deals with the method by which information is transferred. The ninth question asks the respondent to identify the form of disclosure. The tenth question asks the respondent to identify the protection and guarantees provided affected individuals.

A draft of the questionnaire was used in a pre-test carried out with five private firms and five public organizations. We sought to identify firms or organizations that transfer personal data relating to employees or clients and to third parties, in a variety of contexts. We attempted to obtain interviews with people who were up-to-date on these issues. In the public sector, we conducted telephone interviews with two departments, two government boards and one institution of higher education. In the private sector, we conducted interviews with a bank, an insurance company, an agency in the marketing field, a general finance firm and a firm that finances purchasers of a particular brand of durable goods. As a result of the pre-test, we redrafted certain questions and changed the order of presentation.

2 The population

2.1 *Establishing the population*

We sought to establish a population composed of the largest organizations and firms in Canada that were likely, in our view, to transfer significant amounts of personal data, and to send our questionnaire to all these organizations and firms without selecting a sample. We wanted to record the characteristics of a precise population, rather than to select a representative sample from this population. At the beginning of Part 3 we will examine the consequences of this decision.

We established our population from two distinct sources. Relying on our experience, we used lists provided by a market analysis firm. These are the most complete lists in Canada that categorize firms according to the SIC (*Standard Industrial Classification*) in use at the federal Department of Industry, Science and Technology, among other places. For the private sector, we chose the largest firms (50 or more employees) in each sector in which personal data on clients was most likely to be transferred outside Canada. To account for employee files that might be transferred by any type of firm, we asked that 750 of the largest Canadian firms, not already selected in the first operation, also be included.

The public sector population was defined on the basis of two different sources. First, for what we might call the "quasi-public" sector, the firm provided us with a list of all organizations with 100 or more employees, in four fields of activity, for the whole of Canada. These were health services, social services, educational services and municipal governments. Because the target population thus reached was composed primarily of organizations operating at the local level, we used another method to reach the various government departments and centralized organizations likely to transfer personal data outside Canada.

To complete this operation, we used different sources of information for each province. For Quebec and Ontario and for the federal level, we used directories published by each of these governments for the purpose of implementing their respective access and privacy legislation. These directories identify the coordinators or persons responsible for access and privacy for each government department or organization selected. For the eight other provinces, we referred to the 1988 *Corpus Almanac and Canadian Sourcebook*, which lists all government departments and organizations in Canada and identifies the individuals in authority for each. We selected most of the departments of the various governments and a number of public organizations that might have particularly sensitive information on individuals. Because structures vary from province to province, the number of departments and organizations selected varied accordingly. Thus, in some provinces we did not find as many independent agencies as in others. A branch of a department might perform functions that in other provinces are performed by a board.

A detailed breakdown of the firms, quasi-public organizations, government departments and government organizations follows. It includes departments within the federal government and each of the provinces. The codes refer to the SIC categories.

Table 2-1
Public sector population

Government departments and organizations

Governments	Departments	Organizations	Total
Federal	23	11	34
Quebec	25	11	36
Ontario	29	2	31
New Brunswick	16	4	20
Prince Edward Island	13	2	15
Nova Scotia	24	7	31
Newfoundland	23	2	25
Alberta	24	3	27
British Columbia	16	3	19
Manitoba	24	3	27
Saskatchewan	22	4	26
Total	239	52	**291**

Quasi-public organizations, 100 or more employees

SIC CODE		
80: Health services	744	
82: Government educational services	586	
83: Government social services	293	
93: Municipal governments	297	
Sub-total for quasi-public organizations	**1920**	
Sub-total for the public sector		**2211**

Table 2-2
Private sector population

"Target" firms, 50 or more employees

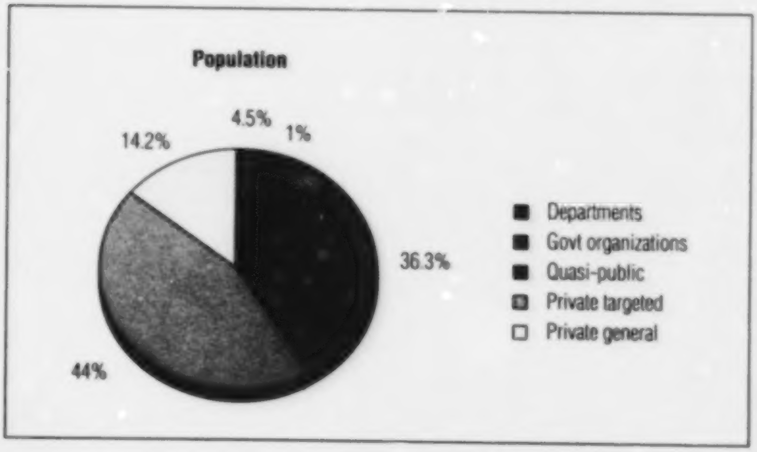
SIC CODE	
2711 and 2721: Publishing & printing, newspapers & periodicals	117
4511: Licensed air carriers	35
4722: Passenger transportation organizations	67
48: Communications	145
60: Banks, trust companies	78
6131, 6142, 6143, 6145, 6146, 6149, 6162, 6163: Credit institutions	95
6281: Services similar to securities brokerages	9
63: Insurers	146
6411: Insurance agents, brokers	102
6531: Real estate agents, brokers, managers	215
66: Insurance/real estate combination	2
7011: Hotels, motels	574
7311: Advertising agencies	50
7321: Consumer credit information bureaus	16
7331: Mail advertising	14
7361, 7362 and 7369: Personnel employment agencies	55
7372, 7374 and 7379: Computer programming, data processing & computer services	153
7393: Detective agencies	115
86: Nonprofit associations	270
8931: Accounting, auditing and bookkeeping services	70
94: International organizations	1
Subtotal for firms "selected for their clientele"	**2329**

Table 2-2
(continued)

Largest firms in the "residual" categories		
0111-0971: Agriculture, forestry and fisheries	1	
1011-1499: Mines	46	
1521-1799: Construction	18	
2011-3999: Manufacturing industries	275	
4011-4971: Transportation, communication and other public services	63	
5012-5199: Wholesale	58	
5211-5999: Retail	87	
6011-6799: Finance, insurance and real estate (except as above)	142	
7011-8999: Services (except as above)	61	
Subtotal for firms in the residual category	**751**	
Subtotal for the private sector		**3080**
TOTAL POPULATION (Tables 2-1 and 2-2)		**5291**

Graphic 2-1 visually illustrates the breakdown of the whole population into these various categories of organizations and firms.

Graphic 2-1
Population of the study



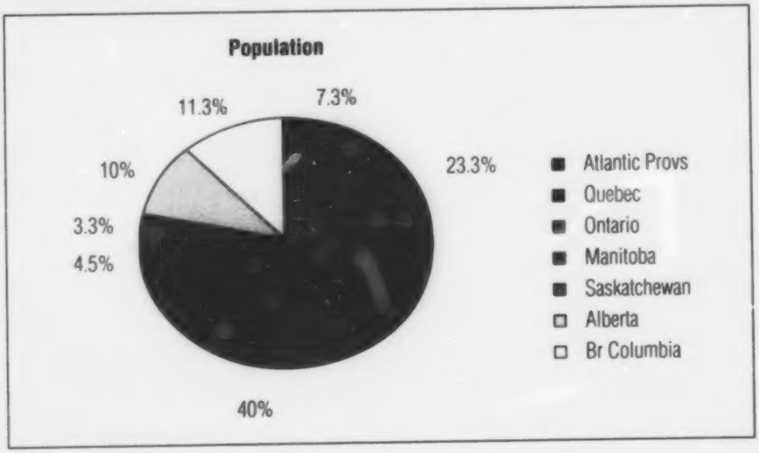
The geographic distribution, by province, was as follows:

Table 2-3
Distribution of the population by province

Newfoundland	101	Manitoba	238
Nova Scotia	146	Saskatchewan	175
Prince Edward Island	31	Alberta	530
New Brunswick	112	British Columbia	596
Quebec	1231	Northwest Terr.	9
Ontario	2115	Yukon	6

This distribution is illustrated in the following graphic.

Graphic 2-2
Population by province



2.2 *Comparison with populations examined in other studies*

The population we examined was one of the largest and most complete ever examined on this issue.

Table 2-4
Population or sample in comparable studies

Study	Number surveyed
OECD 1986 (internationalization of software & CS)	not specified
KANE 1986 (transborder flows, U.S. corporations)	370
SAMBHARYA 1985 (transborder flows, U.S. corporations)	455
EDI Research 1988 (state of EDI in Canada)	500 +
GRID 1985 (private personal data bases)	565
GRID 1988 (personal data transfers)	4788
IBI 1983 (transborder data flows)	5047
GRID 1989 (transborder data flows)	5291

The list of related studies shows that our population of 5291 potential respondents is the largest and is comparable only to the 1983 study by the Intergovernmental Bureau for Informatics (IBI) and the study on the transfer of personal data conducted by GRID in 1988. Other populations or samples were between 370 and 565 or were not specified.

It must also be noted that the composition of these populations varied considerably. The earlier GRID study on the transfer of personal data in 1988 was directed to substantially the same clientele. It covered the same "target" firms and organizations because of their presumed participation in exchanges of data and included certain commercial firms. We replaced commercial firms with the largest private employers in Canada, irrespective of their field of activity (specifically including industry), to assess data flows relating to employment records. Our population in this study also included a larger number of government departments and organizations (291, compared with 100 in the 1988 study).

The study carried out by IBI in Rome (1983) surveyed a comparable number of public and private companies (5,047). The corporations and organizations in more than 125 countries throughout the world were selected from a commercial list. The sample included product and service marketing and distribution companies operating on a worldwide scale but it did not take into consideration the size of the firm, in terms of the volume of business, the number of clients, or the number of employees. Surprisingly, North America was markedly underrepresented in this sample, given its importance in the world economy and particularly in the area of electronic processing and telecommunication of data. Only 300 North American firms were approached. This survey was closest to ours in terms of size. However, the composition of the sample makes it difficult to compare results.

Other studies related to much more limited populations or samples. The 1985 GRID study, which dealt with the general situation relating to private personal data bases, examined a sample of 565 private firms doing business in Quebec. Two other studies were done by universities in the United States, which examined large American and multinational corporations based in the United States and dealing with transborder data flows. The most substantial (Sambharya) dealt with a population of 455 multinationals in the manufacturing industry and service sectors (banks, finance, life insurance, miscellaneous services). The other study (Kane) dealt with 370 large corporations. The report of the 1986 OECD study on software and computer services, targeting professional associations and firms, as well as the 1988 study by EDI Research Inc on the system of electronic data interchange, did not specify the size of their population or their sampling methods.

Our study is among the largest and best distributed, in terms of both geography and fields of activity. It has the advantage of being directed to respondents in only one country, in order to determine the situation in that country, Canada. It takes into account the field of activity of private firms and public organizations, their geographic distribution and their size in terms of employees. Only the largest firms and organizations were selected. The sectors where substantial transfers of personal data are likely to occur were over-represented. Every precaution was taken to obtain the most accurate possible reflection of the Canadian situation in the export of personal data.

3 Questionnaires sent and received

3.1 Questionnaires sent

Of the 5,291 questionnaires sent out on November 1, 1989, 51 were returned to us with incorrect addresses; this represents a rate of error of less than 1%. We therefore had a population of 5,240 recipients of the postal questionnaire. Two reminder letters were sent to all recipients, on November 22 and December 6. In addition, we sent some 50 supplementary questionnaires to those who had lost their copies.

3.2 Questionnaires received

In total, as of January 9, 1990, we received 1,777 completed questionnaires, 387 of which stated that they engaged in transborder data flows ("yeses") and 1,390 that they did not ("noes"). We dealt with these two categories separately. One public organization sent us two replies, one for each of its two subdivisions. One health service took the trouble of sending us seven completed questionnaires, one for each of the programs it administers. We counted each of these questionnaires in our statistics.

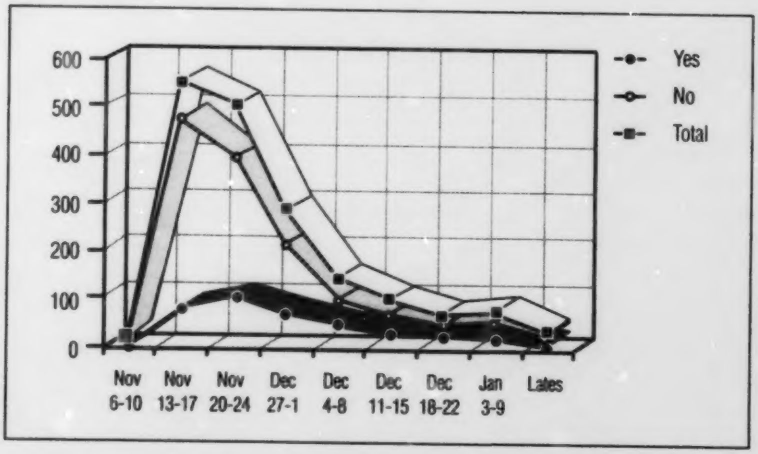
We subsequently received 28 questionnaires (which we will refer to as the "lates") between January 10 and January 22, of which 10 were "yeses" and 18 "noes". We took these questionnaires into account in calculating the rate of response and later, to the extent that they may have made a significant change in our results and influenced our analyses.

The rate at which questionnaires were received is reflected in Table 3-1 and Graphic 3-1.

Table 3-1
Questionnaires received

Week		Yes	No	Total	Cumulative
November	6 -10	5	22	27	27
November	13-17	79	476	555	582
November	20-24	106	398	504	1086
Nov/Dec	27- 1	71	218	289	1375
December	4 - 8	46	102	148	1524
December	11-15	29	73	102	1625
December	18-22	27	46	73	1698
January	3 - 9	24	55	79	1777
Subtotals		387	1390	1777	1777
Lates		10	26	36	1813
Totals		397	1416	1813	1813

Graphic 3-1
Questionnaires received



It may be seen that the rate at which responses were received accelerated in the second week, reached a peak in the third week and then decreased. At the same time, given the ease of answering "no" to the questionnaire, the rate of "yeses" in relation to responses as a whole improved over time. It will also be noted that the private sector exhibited greater haste to reply at the outset while public organizations sent their responses in greater numbers starting in the middle of the period in question.

4 Mail received

We received considerable mail about this survey. Respondents took the study very seriously and were concerned about providing as much information as possible and about being informed about the results. Even a few respondents who do not engage in transborder flows of personal data asked us for a summary of our conclusions. We propose to set out a brief analysis here of the content of the mail we received, which we have separated into nine categories.

4.1 *Simple covering letters (24)*

We received 24 letters informing us that the person in the highest position in the firm or organization, to whom we had sent the questionnaire, had given it to the most knowledgeable person in the firm or organization for reply. In some cases, we were advised that other firms or organizations, under a particular department, for example, were in a better position to reply to the questionnaire.

4.2 *Requests for summary (59)*

Thirty-two firms or organizations indicated that they engage in transborder data flows, and asked us to send them the results of our study. Among those that did not engage in transborder flows, 27 wanted to receive the results. As well, eight organizations sent us separate letters asking for a summary of the results of the survey they had answered. In these cases we could not determine whether they engaged in transborder flows. We thus had a total of 59 respondents who indicated their desire to be informed of the results of the study.

4.3 *Letters explaining responses (18)*

Eighteen respondents took the trouble to attach an explanatory letter to their completed questionnaire. Of these, 11 exported personal data in the fields of education, health, inmate administration, motor vehicle control, foreign missions, life insurance or communications. A missionary group stated that it engaged in personal data flows, but did not answer the questionnaire because of the specific nature of its services. An insurance firm told us it transferred information only on the salaries of senior managers who earn more than $40,000 per year and on the hiring of these managers. Another insurer, the Canadian branch of an American firm, explained that it uses a central computer in the United States for all its operations. All processing is done by direct telecommunications, with the Canadian branch handling all direct contacts with clients. That respondent also transferred information to the Medical Information Bureau in Boston. A public organization described the three subject categories into which its exchanges fall (post box rentals, property claims, accident claims). A government department indicated that it acts as intermediary in some cases and that the consent of individuals is always obtained.

Of the seven respondents that do not engage in transborder flows, three were public organizations. They stated their transactions deal with statistical or tourism data but not personal data. One affirmed that these were interprovincial rather than international flows of information. Another, in the field of education, stated that it occasionally sent personal data concerning teachers or students, but only at the request of those individuals (this comment appeared frequently in questionnaires in this field). A bank stated that it transferred practically no such information, and a computer service firm said it responded only with respect to its own data, not its clients' data. This amounted to almost no transfers since the firm did not engage in transactions of this nature.

4.4 *Documents submitted (25)*

We asked our respondents to send us, if possible, documents that relate to the issues in our study. We received several such documents of various types.

(a) International treaties and agreements
  - List of treaties and agreements concerning a category of people under the organization's administration and explanations submitted in confidence
  - Constitution of Interpol

(b) Statutes and regulations
  - List of legislation applicable to transfers abroad (from a Quebec government ministry)
  - Copies of the British Columbia Hospitals Act and regulations
  - Relevant passages of the Quebec Automobile Insurance Act

(c) Codes of ethics and guidelines
  - Northern Telecom code of ethics
  - General regulations of the Medical Information Bureau (MIB)
  - Departmental guideline concerning disclosure by the RCMP of information on criminal records

(d) Extract from the federal privacy repertory
  - Heading relating to the Department of Supply and Services of Canada

(e) Forms
  - Membership in a real estate agent association (RE/MAX Realty)
  - References for property sale proposal (Century 21)
  - Details on contractors (DKW Systems)

- Verification of foreign nursing licence (professional corporation)
- Teacher exchange (Ministry of Education)
- Consent for medical examination (medical ethics committee)
- Authorization to disclose confidential information (alcoholism commission)
- Security clearance (Government of Canada)

(f) Studies

- Recommendation by the Independent Computer Services Association of Canada to reduce the importation of computer services, submitted to the Parliament of Canada, February 1984
- Analysis by the Independent Computer Services Association of Canada of the economic costs of including communications and computer services in the Canada - United States Free Trade Agreement, submitted to the Parliament of Canada, February 1984

(g) Miscellaneous

- Article by T. Appleby in the Globe and Mail: "Global Strategy Urged in Fight Against Crime"
- OECD News, No. 150, Nov-Dec 1989
- Pamphlet on tracing and family reunification services offered by the Canadian Red Cross Society
- Pamphlet on the Christian Heritage Party of Canada
- Pamphlet on Baptist foreign missions

4.5 *Letters stating that the respondent engaged in no transborder data flows (34)*

We now come to those respondents who, instead of returning the completed questionnaire to us, sent us letters. The first of these categories included respondents reporting they did not engage in transborder personal data flows, either in letters or in questionnaires where the answer "no" was the only entry. There were 34 of these respondents, including those in the following fields: university (1); school board (1); regional school board (1); hospitals (2); institutes of technology (2, one being a medical institute); municipality (1); ministry of housing (1); ministry of labour (1); public service commission (1); provincial health services commission (1); paramedical services agency (1); public hydroelectric production and distribution agency (1); public share and deposit insurance agency (1); association of shipping employers (1); association of wheat producers (1); insurer (1); department store chain (1); mortgage loan company (1); credit cooperative (1); real estate companies (2); manufacturer (1); restaurant chain (1); and travel agency (1).

4.6 *Letters stating that the respondent engaged only rarely in transborder flows*

Seven respondents reported that they engaged in transborder flows of personal data very rarely or that their activity in this regard was too small to be seriously considered in our study. These were: university (1); public rehabilitation agency (1); clinic (1); social services centre (1); seminary for priests (1); institute of chartered accountants (1); and an insurance broker (1).

4.7 *Letters explaining failure to reply to the questionnaire (6)*

Six organizations explained why they did not reply to the questionnaire. One bank explained that its flows were of a financial nature and highly confidential. A college reported it did not transfer anything without the authorization of an adult and that transfers generally were made to foreign universities. Two universities said they disclosed data only with the consent of the persons concerned. A hospital reported it sent data to insurance companies and did not know the disposition of the data. Another hospital said some records follow patients when they are transferred abroad for treatment but always with their consent.

4.8 *Letters stating that the survey was not applicable or not relevant (37)*

There were 37 of these respondents: international agency (which seems very surprising) (1); college (1); school boards (2); elementary school (1); city (1); hospitals (2); ministry of employment (1); ministry of the solicitor general (1); professional institute (1); religious congregations and synagogues (several); artists' association (1); political party (1); union (1); life insurance company (1); car sales firm (1); pharmacy (1); cable television company (1); real estate agency (1); association of real estate agents (1); family company (1); pulp and paper companies (2); hydroelectric commission (1); and an advertising agency (1).

4.9 *Refusal or inability to reply (29)*

These 29 letters are the least interesting. Most refused without explanation. Some stated that the information was confidential. Others did not have the time. Other explanations included reorganization of the firm or of the computer system, shortage of staff, smallness of the municipality or firm. Others had a policy of not responding to surveys. One person confided over the phone that an exception had been made to such a policy in order to respond to our questionnaire. A security agency asked us for $150 to compensate for the time spent answering our questionnaire.

5 Telephone calls received

We were frequently contacted by telephone during this survey. We noted any information that could supplement responses and help us in interpreting the results.

5.1 *Requests for information and clarification*

Several people asked us what the purpose of our study was, and asked questions relating to their own situation.

5.2 *Negative responses (8)*

Some firms or organizations informed us they did not engage in transborder data flows: a city, a social agency, a community centre, a retail merchant, a travel agency, and a computer service bureau that handled all the data for a provincial government. This last agency noted that while it did not engage in transfers itself, it was not aware of whether the ministries and agencies with which it dealt did so.

5.3 *Non-responses (5)*

On several occasions we were told that, in the public sector, disclosure or exchange of data was done with the consent of the person concerned, often at his or her request. We did not believe it advisable to explore this issue with all respondents, even though this made some public sector agencies hesitate to answer "yes" to the question of whether they transferred data. Some other organizations, religious congregations in particular, did not feel our questionnaire related to them. They were kind enough to forewarn us they would not be responding in writing. One firm explained that its computer system was being reviewed by a firm of outside consultants and that it preferred not to respond in the circumstances. Another explained that it preferred not to respond because it was impossible to provide precise figures. Still others, a gas distribution company and a municipality, felt the questionnaire did not apply to their operations.

5.4 *Refusal or inability to reply (8)*

Some respondents said were not interested in responding (1), or it was impossible to do so because the person in charge was away (2).

6 Rate of response to the survey

6.1 *Calculation of the rate of response*

We sent out 5,291 questionnaires. Of these questionnaires, 51 were returned unopened, so 5,240 presumably reached their destination. We were not able to identify the sectors of our population to which these cases belonged, so that we will include them in our sector-by-sector analyses, with the understanding that, on average, the rate of response will be calculated on 99% of the population.

Indications of refusal or inability to respond for whatever reason amounted to 29 letters and eight telephone calls, for a total of 37, representing about 0.7% of the sample. We did not include these expressions of refusal or inability to respond in calculating the rate of response.

If we take only those questionnaires that were received as of January 9, 1990, and processed, our rate of response was 33.6%, a little more than one third of the population contacted. If we include the questionnaires received late (1,813), the rate is 34.6%. When we also include in the responses received the letters providing us with a precise answer (34 "no" and 50 "non-responses") and the telephone responses (8 "no" and 50 "non-responses"), we arrive at a total of 1,910 responses out of 5,240 questionnaires sent out, a rate of 36.4%.

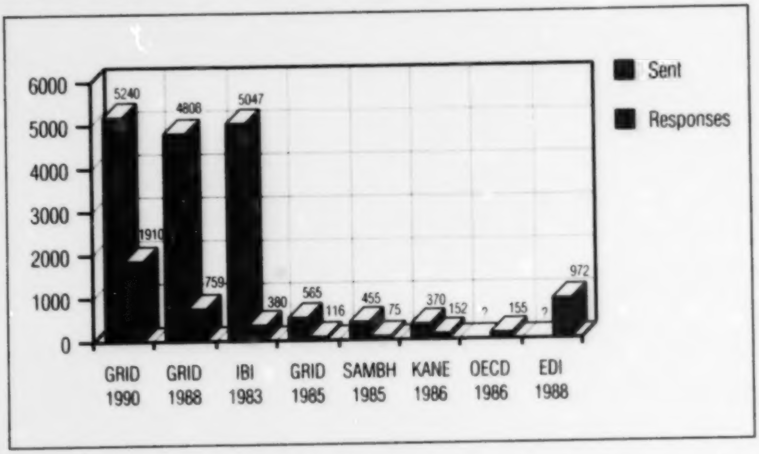
6.2 *Comparison with response rates in the other studies*

The rate of response was comparatively very high. A good rate of response for postal questionnaires is theoretically between 10% and 20%, except in cases where a group with a high level of interest is contacted (such as the members of an association) or where those contacted are obliged to respond. The response was particularly significant in view of the large size of the population. A comparison with studies done in our field provides the following data, set out in Table 6-1 and illustrated in Graphic 6-1.

Table 6-1
Rate of response in comparable studies

Study #	Sent	Responses	(%)
GRID 1985 (private personal data bases)	565	116	(20.5)
GRID 1988 (personal data transfers)	4808	759	(15.8)
IBI 1983 (transborder data flows)	5047	380	(7.5)
SAMBHARYA 1985 (transborder flows, U.S. corps)	455	75	(17)
KANE 1986 (transborder flows, U.S. corps)	370	152	(41)
OECD 1986 (internationalization of software & CS)	not stated	155	(?)
EDI 1988 (state of EDI in Canada)	not stated	972	(?)

Graphic 6-1
Rate of response in comparable studies



In order to comment briefly on these comparisons, we would note the following factors:

1. Our two earlier studies (GRID 1985 and 1988) dealt with broader subjects than were at issue here: i.e., private personal data banks and transfers of personal data. It will be noted that with a smaller sample (565 Quebec firms) and despite the fact that this sample was composed exclusively of private firms, we obtained a higher rate of response to the first survey (20%) than to the second, nearly (16%) where the population was larger (4,808) and broader (public and private sectors in Canada). These figures indicate that the larger the sample, the lower the rate of response in comparable studies.

   An objection to this interpretation might be that the first study, originating in a Quebec university, was addressed exclusively to Quebec firms while the second, from the same institution, covered all of Canada. However, the responses from the other Canadian provinces accounted for 71% of the total, which seems to minimize the importance of the regional factor. In view of these earlier studies, we expected to obtain a rate comparable to that obtained in 1988. Since our population was substantially the same in size and composition, the response rate was quite surprising.

2. The 1983 study by IBI in Rome involved a comparable number of public and private companies (5,047). This study obtained a response rate of 7.5%, which is about five times lower than ours. Although it dealt with the same subject, the scope was probably narrower in 1983 than in 1989. The corporations and organizations, selected from a commercial list, were spread throughout the world. These companies were probably less interested in responding to such a survey by the IBI than are Canadian firms and organizations

who must have felt more affected by a survey done on behalf of the Government of Canada.

3. Two other studies of transborder data flows involving large American corporations and multinationals based in the United States have been conducted by universities. These studies were not designed to analyze practice but to gather opinion on the subject. The response rate for the most substantial study (Sambharya), dealing with a population of 455 multinationals, was 17%, which is considered to be very acceptable for a university study. Obviously, however, the limited number of respondents (75) prevented the author from drawing certain conclusions. The other study (Kane) was much less ambitious, dealing with a still smaller population: 370 corporations. Its high response rate was undoubtedly owing to the fact that the response involved checking off five opinion questions on a one-page questionnaire. The suggested time frame was two minutes.
4. The OECD did an opinion survey on a subject that was different but related to computers. It involved an international issue: the internationalization of computer software and computer services. The results were based on 155 responses received, but the 1989 report does not mention the size of the population. The same was true of the study by EDI Research Inc, dealing with the system of electronic preformatted data interchange. It involved 972 responses to a questionnaire distributed to an unspecified number of firms. The circumstances and the methodology used were not explained.

6.3 *Explanation of the rate of response*

We accordingly assert, on the basis of these comparisons, that the rate of response observed in this study was exceptional. We suggest the following five factors in explaining this rate:

1. We note the interest in this subject and concern on the part of the respondents, as shown by the number of letters and telephone calls. Is this an interest in privacy protection or in the international aspect of the problem? Is it owing to the use of computers and telecommunications? It may be that the corporations and organizations we contacted, the largest in terms of number of employees, were more interested in these questions than smaller firms. The rate may have been owing to the fact that larger firms are technically better equipped and are dealing with transborder flows more frequently, because of the rapid development of computerization and of communication networks.
2. The fact that this survey was conducted on behalf of the Government of Canada, as mentioned in the letter of introduction, may have played a role. This sponsorship indicated the seriousness of the study and suggested that concrete action might be taken in terms of government intervention or nonintervention in this area.

3. We should also mention the quality of the presentation of the personalized letter that accompanied the questionnaire. Respondents felt that they had been called upon personally and this yielded a very large response by telephone and letter. In the earlier study in 1988 on data transfers, we used mailing labels and form letters. The rate of response was half the rate achieved in this study.

4. Sending the two reminder letters, at intervals of three and five weeks after the questionnaire was sent, may also have had an effect. The statistics referred to in point 3.2 show the rate at which responses were received. The reminder letters undoubtedly helped in eliciting a large number of responses. In particular, the second reminder letter sent on December 6 resulted in about 50 requests for questionnaires. If we estimate that half the responses received one week after a reminder letter were a direct result of the reminder, we can say that about 350 questionnaires, or 20% of the total, were sent following receipt of one of these two letters.

5. Finally, we would note the relative ease of responding only to the first page of the questionnaire, when there were no transborder flows. By drafting the questionnaire in this way we were able to gather considerable data on the proportion of firms and organizations (80%) that do not engage in transborder personal data flows. This information includes the number of such firms, size (clients, employees) and jurisdictions.

The rate of response greatly exceeded all predictions and our most optimistic expectations. We can rely on more than 1,800 questionnaires, giving us information on whether transborder personal data flows occur, by field of activity and jurisdiction. Of these, nearly 400 respondents engaged in transborder data flows. They provided us with a detailed and most illuminating description of this activity.

7 Coding and analyzing data and preparing tables

7.1 Coding

This operation consisted of determining the content of the responses to each question and deciding how to code the open questions. We were able to consolidate this coding plan, as necessary, in two ways: 1) by assigning new categories for the open responses and 2) by making decisions as to how to code the responses so that they could be recorded in either the predetermined categories or in a new category. We used this process to note all the marginal comments that the respondents might have written on the questionnaire.

This coding process has been described in detail in a document entitled *Description des variables et des valeurs*. The variables represent the questions that were asked and answered, while the values represent the various possible responses to a single question. We later decided to divide our questionnaires into four sets, so that we could more easily sort them by large sectors and process them separately. This decision proved to be correct when we later agreed to process the "yeses" and "noes" separately for statistical purposes.

The receipt of 14 questionnaires from respondents who had answered "yes" to question 2, without then going on to respond to the rest of the questionnaire, led to the creation of a fifth category. This response may be explained in four ways: the respondent did not understand the meaning of the question; the respondent checked "yes" in error, intending to check "no"; the respondent answered "yes" to the first question and, in answering "no" to the second, believed in error that he or she should immediately return the questionnaire (this seems to be the most plausible explanation); or, finally, the respondents were indicating they engaged in transborder flows but did not want to provide the details requested in the questionnaire. For these few specific cases, as for the "lates", we did no computerized statistical analysis. We verified that the cases did not contain anything exceptional in relation to the other responses received. We did include them in calculating our response rates but we did not refer to them subsequently.

7.2 *Determining the activity and sector of activity*

It is important to explain here in detail the strategy of the questionnaire and the coding under these two headings, as set out in questions 1a) and 1b) of the questionnaire, appended to this report. We had learned from experience that firms and public organizations do not always describe or categorize themselves in the same way as we would. There is no objective way of classifying the activities of firms or organizations. We therefore chose to ask them first (question 1a) to describe their principal activity themselves and second, (question 1b), to classify themselves in one of the 15 categories that we had established. We hoped thus to minimize uncertainty by permitting cross-checking between questions 1a) and 1b).

For question 1b), we established 10 categories in the private sector and five in the public sector. We had to create "logical" groupings to analyze them statistically, given the diversity of types of activity, particularly in the private sector but also among government departments and agencies. For question 1a), to allow for some refinement, we used a finer breakdown of 45 categories, including one "undetermined". In some cases, this was the basis on which we grouped certain categories for statistical purposes.

Several typical cases arose in sorting the questionnaires. Most of the firms and agencies described themselves appropriately and coherently in 1a) and 1b): for example, "life insurance" in 1a) and "insurance" in 1b). However, some wrote nothing in 1a) or wrote something general and not very helpful (e.g. "service to the public"). In these cases we then had to supplement their answer by reconciling it with the response given to 1b) and, in some cases, by looking at the answers to other questions (for example, the uses of, or nature of, the data transferred) to classify these respondents with greater certainty. In cases where we could not reasonably do so on the basis of this information, we left this respondent as "undetermined". However, because the field of activity was vital to our analysis, we made a strong effort to fit all our responses into the appropriate categories.

We could attempt a few explanations as to the vague responses or non-responses found in classifying the activities and sectors of activity. It was obvious that a few respondents had not understood the meaning or purpose of the question and so answered in general terms. Others undoubtedly wanted to preserve the confidentiality of their responses by not identifying of their activities precisely, particularly in sectors where they were almost the only ones operating.

In any event, we proceeded in the same way in coding the responses to question 1b). In some cases where no response was provided, we took the initiative by entering a response that was consistent with the statement in question 1a). In other cases, when the entry in 1b) did not agree with the response in 1a), we changed it accordingly. We also found several cases where multiple answers were given. Some respondents believed that we were asking them for the economic sector in which they offered their services and so checked several boxes. For example, a computer services firm checked every answer, because it offered services to industry, insurers, municipalities and so on. Since the intention of this question was to assign a firm or organization to a single category among these sectors of activity, we therefore had to choose from the multiple responses by selecting the aspect that appeared to us to be most important for classification purposes. These choices are explained below.

It is therefore important to note that the code we assigned to the responses to questions 1a) and 1b) does not necessarily correspond to the literal description given by the respondent; rather, it is the result of comparing the responses to questions 1a) and 1b) and to other questions, if necessary, to decide on the best possible approximation in vague cases.

We would also note that all our categories are mutually exclusive for statistical reasons. Thus, firms or organizations involved in many sectors or activities were assigned to a category on the basis of their dominant activity. Each respondent was therefore assigned to only one category of activity in response to question 1a) and to only one subsector of the private or public sector, as the case might be. It was not possible for them to belong to two categories because we wanted to avoid double counting. Respondents whose characteristics were undetermined (code 99), which we were not able to assign even to the private or public sector, or whose description was vague or ambivalent, were classified in the "other" category of the private sector for question 1b).

7.3 *Preparing the statistical tables*

In establishing the list of computerized tables to be compiled from the data collected, our first decision was to deal separately with the "yes" and "no" respondents. We did this because only the first question could be used for cross-tabulating.

For each of the sets ("yes" and "no") we asked for 16 frequency tables to be created: one for all respondents (A), one for the public sector (B), one for the private sector (C), and one for each of a number of subsectors, or groups of subsectors, based on our categories and the responses received. The tables requested were integrated into two broad general compilations (for the "yes" and "no" responses) so that we could do horizontal question-by-question comparisons among sectors. The results of these tables will be presented in the analysis set out in the third part of our report.

8 Definition of sectors, groups of sectors and subsectors

Within our groups of sectors or fields of activity we have rearranged our subsectors by adapting the SIC to our particular needs. In doing this, we attempted to retain the first two numbers in the classification (for example, 86 = associations). However, we broke down some sectors by assigning numbers to them that are not used in the SIC. In the following paragraphs we provide, first for the public sector and then for the private sector, a description of what is included, adding our own comments where necessary. We will proceed in the order set out in the subquestions in question 1b), listing under each category the subcategories taken from question 1a).

8.1 *The private sector*

1 - ASSOCIATIONS

86 - Nonprofit associations

This category includes all types of associations: professional bodies, religious congregations, religious institutions, unions, associations of organizations or firms, private clubs, agencies offering consulting or animation services.

2 - INSURANCE

63 - Insurers

Includes insurers (with no further details), general insurance, life insurance and health insurance, and may extend to cover pension funds and annuity management firms.

64 - Insurance agents

Includes disaster experts and miscellaneous services directly related to insurers (indexes, statistics) but does not include computer services (category 75).

3 - RETAIL/WHOLESALE BUSINESS

50 - Wholesale business

We included not only wholesalers but also those who stated that they are in both the wholesale and retail business. Some respondents operate in both the food and wood products sectors. When a manufacturer also markets its products, we included it in the "industry" (20) category.

52 - Retail business

Includes retail businesses, from department stores to restaurant chains. We selected about 1,000 firms, among the largest in Canada in terms of numbers of employees, indicating that we are dealing here with very large commercial organizations.

59 - Undetermined

Includes businesses that we were unable to classify with certainty in 50 or 52.

4 - COMMUNICATIONS

27 - Publishing and printing

Includes firms that publish newspapers and periodicals, printers and distributers.

48 - Communications (in general)

Includes communications firms in general, with the exception of those in the preceding category. In particular, it includes telephone services, data communication services and electronic publishing.

5 - FINANCE

60 - Banks

This category comprises financial institutions engaged primarily in banking. With the diversification of financial institutions, there is increasing complexity in the operations of many firms in the financial sector. We have included savings and loans organizations, credit cooperatives, caisses populaires and credit unions in this category. Trust companies are in a separate category (68).

61 - Credit institutions - other

Includes "finance companies" and other lenders.

62 - Securities brokers

65 - Real estate

Includes real estate promoters, property owners and real estate services but not real estate agents.

66 - Real estate agents

In addition to agents we included a multiple listing service that is closely connected to this sector.

67 - Investment companies

Includes investment companies dealing in portfolios.

68 - Trust companies

69 - Finance (undetermined or composite)

Along with firms in the financial sector, which we were unable to classify because of a lack of information, we included firms with multiple activities that did not seem to have one dominant activity.

72 - Credit bureaus

We included credit bureaus in the finance sector, given the close ties between such bureaus and credit institutions.

6 - INDUSTRY

10 - Primary

We included agriculture, natural resources (particularly forestry) and energy (particularly petroleum) - in short, the "primary sector" of economic analysis.

15 - Construction

20 - Manufacturing industry

We placed all manufacturing industries in this category, including those which market their own products. It includes steel, food, cars, machinery, diagnostic equipment, electronics, engineering products, systems engineering, pulp and paper, wood products, petrochemicals, shipbuilding.

49 - Public services

Includes firms (and organizations or publicly owned corporations) that distribute water, gas or electricity or remove garbage. These are not services provided primarily by municipalities.

7 - TRANSPORTATION AND TOURISM

40 - Transportation in general

We provided only one category for transportation and tourism, in which we included one recreational firm. We included in this category all organizations relating to land and sea transportation, excluding air carriers and travel agencies.

45 - Air transportation

Includes aerospace transportation (one case).

47 - Transportation organizations

In addition to travel agencies, we included auto clubs, travelers' aid services (health and so on) and two firms that checked off the categories: "Retail/Wholesale" and "Transportation and tourism".

70 - Hotel services

In addition to hotels, we included organizations that relate to tourism in general and that are often part of hotel complexes like skiing and recreational facilities, restaurants, resorts.

8 - BUSINESS SERVICES

This broad category covers services offered to both private businesses and public organizations.

71 - Advertising agencies

Includes marketing services but not direct marketing.

73 - Mail advertising

Includes direct marketing.

74 - Personnel employment services

75 - Computer services

Includes all kinds of computer services: general services, systems development, systems integration, systems and software marketing, software sales, equipment maintenance, data processing in general, data base production, payroll processing, electronic transactions and consulting.

76 - Security

Includes detective agencies and security firms.

77 - Collections

Includes debt collection agencies.

88 - Accountants

Includes chartered, public and general accounting firms and management and accounting consultants.

89 - Miscellaneous professional services

We grouped together professional services such as consulting engineers; management and technology consultants; administrative advisers; research and development firms; and purebred dog registration. We had a problem in interpreting this last example, because it was not clear whether the information transferred (such as registration of the dog abroad and language of communication) related to the animals or their owners.

0 - OTHER

94 - International organizations

There was only one such organization with a head office in Canada in our sample. Because it was a private organization, we classified it under the heading "other" in the private sector.

99 - Undetermined

This category may be found in the other sectors referred to but it is concentrated under our "other" heading which, in this case, refers to both the private and the public sectors. For example: a firm that entered only "entertainment" in question 1a) was classified under "other - undetermined". Another respondent was so multifaceted that it was not possible to assign it to any sector (it had replied "manufacturing & distributing & hotel services"). The other respondents in this category gave no response to either question 1a) or question 1b) that would permit us to classify them otherwise.

8.2 The public sector

1 - EDUCATION

82 - Education

Includes school boards, colleges and universities, whether public or private. Because most of these organizations are heavily subsidized by the government and belong to the same network for circulating personal data as the public organizations, we included them in the public sector.

2 - MUNICIPAL

93 - Municipality

Includes cities or "local government". When the only information we had covered both "municipal" and "education" we included the entry in "municipality" (2 and 93) because schools are directly under the control of the municipalities.

97 - Municipal organization

Includes organizations connected with the municipal sector: police departments; electric utilities; libraries; promotion of the natural and historic resources of the Toronto region; urban mass transit organizations; water utilities; municipal water and electric utilities.

3 - HEALTH AND SOCIAL SERVICES

80 - Health

Includes hospitals or medical centres, medical research centres, centres providing care for the disabled, including both public (as most are) and private (for the same reasons as in the education sector).

83 - Social services

Includes social services when identified as such; social service centres; group homes; family services; a centre that promoted "independence for adults suffering from a physical handicap".

84 - Health and social services

We created a specific category to include organizations of the same type as those in 83 but which specified they offered health care; for example: a local community service centre in Quebec. Also included were organizations that did not respond to question 1a) but checked off "Health/welfare" in question 1b).

4 - GOVERNMENT DEPARTMENTS

When a public organization identified itself as a government department, we included it in the "government department" category to distinguish it from other sectors of activity (education, municipal or health and social services) and from other government organizations. The activities of government departments involve a number of sectors of activity. However, rather than submerging them in the broader quasi-public categories, we preferred to identify them by their place in the government structure and distinguish them from other organizations that are not necessarily subject to the same operating rules. We therefore included in this category some fairly disparate organizations. The commonality was that they were departments of the federal or provincial governments.

91 - Federal department

92 - Provincial department

Some organizations identified themselves as a government department, undoubtedly because they considered themselves to be a division of a department and not an autonomous agency. We respected this choice. These organizations were a motor vehicle bureau; a corrections and police agency; an agency regulating the sale and transportation of alcohol; and an insurance regulating agency.

5 - OTHER ORGANIZATIONS

95 - Federal organization

Includes an organization for the "promotion of leadership by the federal government in the democratic process"; a development commission; an Indian band; and a public security service for Indian communities.

96 - Provincial organization

Includes a motor vehicle bureau; a workers' compensation board; an occupational health and safety board; an agency serving adult vocational training needs and programs; a Crown corporation offering computer services; a Crown corporation administering automobile and general insurance in a province; another offering electrical power production services; an administrative tribunal or regulatory agency; a pension plan administration agency; a housing agency; organizations involved in scientific research, environmental protection, leisure, sport and hunting; health and social services; an industrial development corporation; a small business assistance agency; an energy agency; a crop insurance agency; a construction industry administration agency; and a sheltered workshop.

9 Rates of response by sector and group

We saw in Section 6 the rates of response obtained for the survey as a whole. We will now analyze these rates of response, looking first at the variations between the public and private sectors and then examining the distinctions between both the groups of subsectors and each subsector. We can thus understand the composition of the groups, in terms of the population surveyed and the number of respondents.

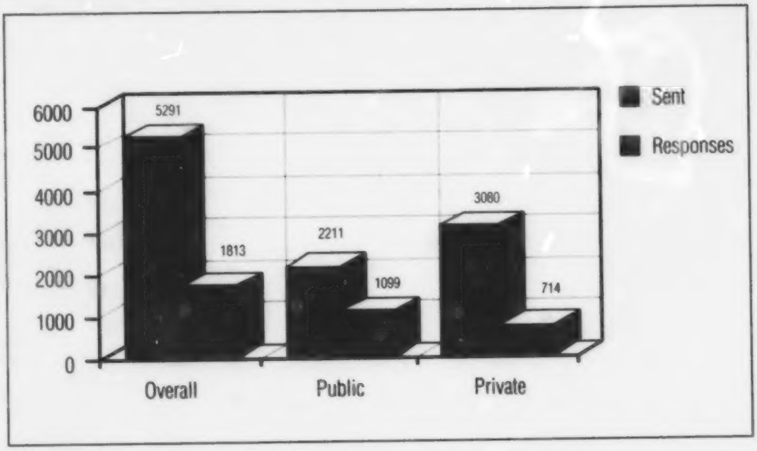
9.1 *The rate of response overall and by sector*

Table 9-1 and Graphic 9-1 indicate (both for respondents as a whole and for each of the public and private sectors) the number of questionnaires sent out and the number of responses received, by whether or not ("yes" or "no") there were flows of transborder personal data. The percentages represent, in turn: rate of response by sector and proportion of "yes" and "no" replies for respondents in each sector. The last two percentages will total 100% of the respondents in each sector).

Table 9-1
Rates of response overall and by sector

Sector	Population	Responses (%)	"Yes" (%/R)	"No" (%/R)
TOTAL	5291	1813 (34)	397 (22)	1416 (78)
PUBLIC SECTOR	2211	1099 (50)	219 (20)	880 (80)
PRIVATE SECTOR	3080	714 (23)	178 (25)	536 (75)

Graphic 9-1
General and sector rate of response



We will first consider the results for the private and public sectors overall. It will be noted from Table 9-1 that the rate of response for the private sector as a whole (23%) is considerably lower than for the public sector (50%). This was to be expected. From our experience at GRID, although we had achieved a response rate of 20% from the private sector in our first study on private personal data bases in Quebec (1985), this was undoubtedly a result of the fact that our sample was small (565) and our respondents less broadly defined (firms doing business in Quebec). In our second study in 1988 dealing with a comparable population (4,808 organizations and firms located in Canada), the response rate, in terms of usable questionnaires, was 17.3% for the public sector and only 4.3% for the private sector, or about one quarter of the public sector response rate. We should note that we were concerned in that study with the problem of computer matchings, which was more of an issue in the public sector.

9.2 *Results for public sector groups*

We combined the subsectors comprising the public sector into broader groups, as defined in the preceding section (Section 8). Table 9-2 provides the figures for the rates of response in the public sector.

Table 9-2
Rates of response by public sector group

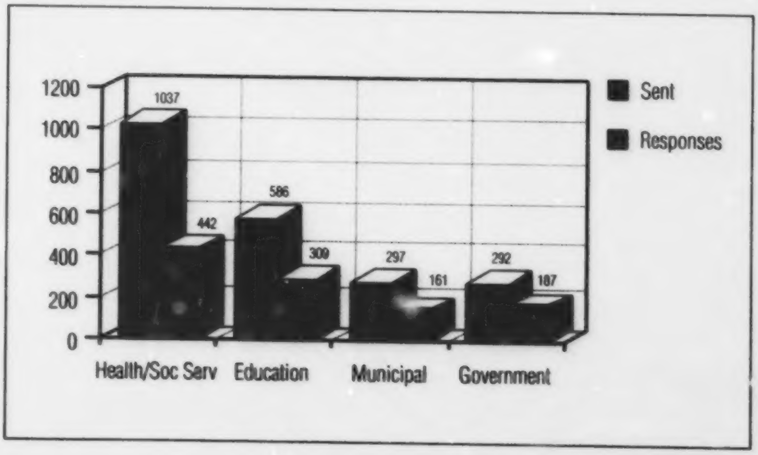
Sector	Population	Responses (%)	"Yes" (%/R)	"No" (%/R)
1. Education	586	309 (53)	78 (25)	231 (75)
2. Municipal	297	161 (54)	10 (6)	151 (94)
3. Health/soc services	1037	442 (43)	88 (20)	354 (80)
4. Departments	239	131 (55)	28 (21)	103 (79)
5. Other organizations	52	44 (83)	13 (26)	31 (74)
0. Undetermined		12 (und)	2 (17)	10 (83)

In view of these results, we grouped "Departments" and "Other organizations" together in one subsector group, the "Government" group. We also reclassified our public sector groups accordingly, designating them by capital letters (P, Q, R, S), as shown in Table 9-3 and Graphic 9-2, arranged in ascending order by rate of response.

Table 9-3
Rates of response by public sector group

Sector	Population	Responses (%)	"Yes" (%/R)	"No" (%/R)
R. Health/soc services	1037	442 (43)	88 (20)	354 (80)
P. Education	586	309 (53)	78 (25)	231 (75)
Q. Municipal	297	161 (54)	10 (6)	151 (94)
S. Government	292	187 (64)	43 (23)	144 (77)

Graphic 9-2
Public sector rate of response



The rate of response was highest in the public sector (average 49%). The fact that the rate for the health and social services group was the lowest (43%) is undoubtedly due to the large size of the group (1,037) and the number of organizations that also employ large numbers of people. Educational institutions and municipalities replied at a slightly lower rate than the average, while government organizations and departments took first place with a response rate of 64%.

Because we do not have a stratification of the populations in each subsector and group of subsectors, we cannot calculate the statistical significance of the preceding figures. It is therefore not necessary to weight our groups on the basis of their size and the observed response rates to establish to what extent they are probably representative, something that could not be demonstrated. However, we can reasonably state at this point that the response rates for each group of sectors is sufficient to provide a basis for a reasonably accurate description of current practice.

9.3 *Results for private sector groups*

The results for the groups of private sector subsectors that we listed in our questionnaire are set out in Table 9-4.

Table 9-4
Rate of response by private sector group

Sector	Population	Responses (%)	"Yes" (%/R)	"No" (%/R)
1. Associations	270	80 (30)	29 (36)	51 (64)
2. Insurance	250	85 (34)	27 (32)	58 (68)
3. Business (Ret/Whol)	145	32 (22)	5 (16)	27 (84)
4. Communications	262	81 (31)	13 (16)	68 (84)
5. Finance	555	84 (15)	19 (23)	65 (77)
6. Industry	340	81 (24)	28 (35)	53 (65)
7. Transport/Tourism	739	135 (18)	12 (9)	123 (91)
8. Services	518	113 (22)	37 (33)	76 (67)
9. Other-undetermined	1	23 (und)	8 (35)	15 (65)

In view of these results, we have, for purposes of statistical analysis, grouped together the "Business (Retail/Wholesale)" and "Industry" categories. We have separated "Computer services" and Professional services" from the "Services" subsector, and created independent categories for analysis of these groups. We also grouped together "Other" services in the category "Miscellaneous services". The firms that we could not classify are found in category O: "Other", and subsector 99: "Undetermined". This category will be counted in compiling data for the private sector as a whole but it will not be analyzed as a sector group.

We will from this point use capital letters to designate our new sector groups (from D to O). For some groups (M: "Professionals"; N : "Misc services") and for the category "Other" (O), the population is difficult to determine because we could not establish, from the responses given, the specific sector to which the respondents belonged. The various occupations that appear in each of these categories are described in detail in Section 8. Our comments concerning the significance of the results for the public sector apply as well to the analysis of the private sector response rate. The rates of response for these new groups are shown in ascending order in table 9-5:

Table 9-5
Rates of response by private sector group

Sector	Population	Responses (%)	"Yes" (%/R)	"No" (%/R)
H. Finance	555	84 (15)	19 (23)	65 (77)
N. Misc services	234	41 (18)	10 (24)	31 (76)
K. Transport/Tourism	739	135 (18)	12 (9)	123 (91)
L. Computer services	153	35 (23)	13 (37)	22 (63)
F. Business/Industry	485	113 (23)	33 (29)	80 (71)
M. Professionals	131	37 (28)	14 (38)	23 (62)
D. Associations	270	80 (30)	29 (36)	51 (64)
G. Communications	262	81 (31)	13 (16)	68 (84)
E. Insurance	250	85 (34)	27 (32)	58 (68)

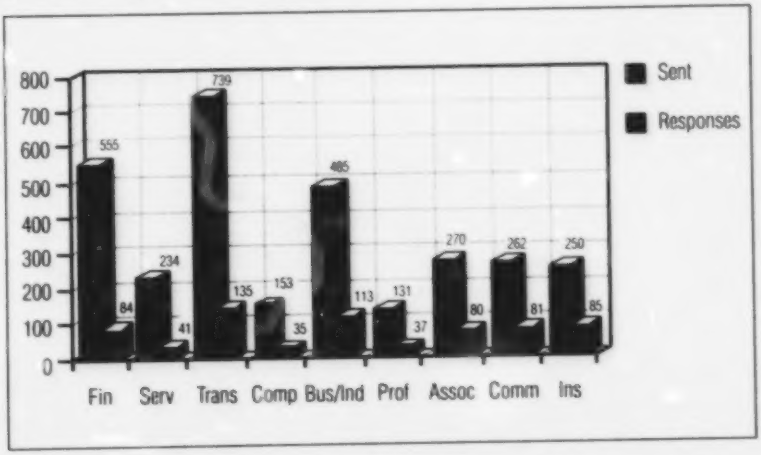
It should first be noted that the lowest response rate was in the finance sector (15%). This is 35% lower than the average private sector response rate and we can rightly deplore the fact that in so sensitive a field these firms did not show greater interest in responding. Fortunately, our population was quite large (555) so our 84 respondents constitute a fairly substantial group. We will see in point 10 how this group breaks down and what variations there were in the rate of response from one subsector to another.

Miscellaneous services, covering advertising, personnel and security agencies, follows with an 18% response rate that is still well below the overall average. The transportation and tourism group also showed a low response rate (18%), probably because of the relatively large proportion of hotels in our population (574). This industry employs a large labour force, which makes it a relatively large component of our population, based on size in terms of number of employees. Contrary to our expectations, hotel services seem still to be relatively local in nature. International reservation systems must still not be too common, judging by our results. Nonetheless we have 135 respondents in this group, which will permit a meaningful analysis of the results.

The computer services subsector and the business and industry group showed response rates corresponding to the private sector average (23%). Professional services and associations exceeded the average by 5 and 7 points (28% and 30% respectively), while communications (31%) and insurance (34%) attained the overall public and private sector response rate.

Graphic 9-3 provides a visual illustration of these results.

Graphic 9-3
Rates of response in the private sector



As may be observed, the response rates vary considerably from one group to another within the private sector. The figures for the fields of finance, miscellaneous services and computer services are relatively disappointing given the importance of personal data in these types of activities. They are, on the other hand, satisfactory in business and industry, and much more substantial for professional firms, nonprofit associations, communications and insurance.

To refine our interpretation, we will arrange the detailed results by subsector composed of the groups that we established for purposes of our statistical analysis. By examining the composition of each group we will be able to extract the results that deserve our attention.

10 Rates of response by subsector

10.1 Tabulated results

The following tables set out the rates of response for each subsector included in the sector groups examined, following the order that we will use in analyzing the data. We will use these tables to compare the total figures (including "lates" and incomplete responses) indicated in italics. The figures obtained from our statistical compilation on the basis of the questionnaires that were processed (i.e. those received by January 9), are indicated in regular print to determine whether there are significant differences by subsector.

Table 10-1 sets out the response rates for the private sector; Table 10-2 for the public sector. For ease in reading these tables, note that in the example of associations, the letter D refers to the subsector group (here there is only one). The figure 1 relates to the code assigned for the response to question 1b), which response was used to establish categories within the public and private sectors before the group was created. (For example: in the private sector, "Business" and "Industry" are separate and are numbered 3 and 6 respectively; in the public sector, "Departments" and "Public organizations" are separate and are numbered 4 and 5 respectively.) The figure 86 designates the category of subsectors we used for question 1a), based on the SIC. The notation "(und)" (undetermined) means that the number in question cannot be determined.

Table 10-1
Rates of response by private sector subsector

Sector	Popul.	Resp. (%)	"Yes" (%/R)	"No" (%/R)
PRIVATE SECTOR	3080	714 (23)	178 (25)	536 (75)
D. Associations	*270*	*80 (30)*	*29 (36)*	*51 (64)*
D. Associations	270	74 (27)	26 (35)	48 (65)
1- 86 Nonprofit Assoc	*270*	*80 (30)*	*29 (36)*	*51 (64)*
1- 86 Nonprofit Assoc	270	74 (27)	26 (35)	48 (65)
E. Insurance	*250*	*85 (34)*	*27 (32)*	*58 (64)*
E. Insurance	250	83 (33)	25 (30)	58 (70)
2- 63 Insurer	*148*	*70 (47)*	*25 (32)*	*45 (68)*
2- 63 Insurer	148	69 (47)	24 (32)	45 (68)
2- 64 Insurance agent	*102*	*11 (11)*	*2 (18)*	*9 (82)*
2- 64 Insurance agent	102	10 (10)	1 (10)	9 (90)
2- 99 Undetermined		*4 (und)*		*4 (100)*
2- 99 Undetermined		4 (und)		4 (100)
F. Business/Industry	*485*	*113 (23)*	*33 (29)*	*80 (71)*
F. Business/Industry	485	110 (23)	31 (27)	79 (73)
3- 50 Wholesale	*58*	*9 (16)*	*3 (33)*	*6 (67)*
3- 50 Wholesale	58	8 (14)	2 (25)	6 (75)
3- 52 Retail	*87*	*18 (21)*	*2 (11)*	*16 (89)*
3- 52 Retail	87	18 (21)	2 (11)	16 (89)

Table 10-1
(continued)

3- 59 Und Ret/whol business		*3 (und)*		*3 (100)*
3- 59 Und Ret/whol business		3 (und)		3 (100)
6- 10 Primary	*47*	*14 (30)*	*6 (43)*	*8 (57)*
6- 10 Primary	47	14 (30)	6 (43)	8 (57)
6- 15 Construction	*18*	*3 (17)*		*3 (100)*
6- 15 Construction	18	3 (17)		3 (100)
6- 20 Manufacturing	*275*	*56 (20)*	*21 (38)*	*35 (62)*
6- 20 Manufacturing	275	55 (20)	20 (36)	35 (64)
6- 49 Public services		*3 (und)*		*3 (100)*
6- 49 Public services		2 (und)		2 (100)

G. Communications	*262*	*81 (31)*	*13 (16)*	*68 (84)*
G. Communications	262	77 (29)	10 (13)	67 (87)
4- 27 Publishing	*117*	*29 (25)*	*7 (24)*	*22 (76)*
4- 27 Publishing	117	28 (24)	6 (21)	22 (79)
4- 48 Communications	*145*	*52 (36)*	*6 (12)*	*46 (88)*
4- 48 Communications	145	49 (34)	4 (8)	45 (92)

H. Finance	*555*	*84 (15)*	*19 (23)*	*65 (77)*
H. Finance	555	81 (15)	17 (21)	64 (79)
5- 60 Banking	*78*	*17 (22)*	*5 (29)*	*12 (71)*
5- 60 Banking	78	17 (22)	5 (29)	12 (71)
5 -61 Other credit	*95*	*2 (2)*		*2 (100)*
5 -61 Other credit	95	2 (2)		2 (100)
5- 62 Securities	9	0 (0)		
5- 65 Real estate		*11 (und)*	*1 (9)*	*10 (91)*
5- 65 Real estate		10 (und)		10 (100)
5- 66 Real estate agent	*215*	*18 (8)*	*5 (28)*	*13 (72)*
5- 66 Real estate agent	215	18 (8)	5 (28)	13 (72)
5- 67 Investment company		*5 (und)*	*1 (20)*	*4 (80)*
5- 67 Investment company		5 (und)	1 (20)	4 (80)
5- 68 Trust company (see 60)		*3 (und)*		*3 (100)*
5- 68 Trust company (see 60)		3 (und)		3 (100)
5- 69 Finance undetermined	*142*	*27 (19)*	*6 (22)*	*21 (78)*
5- 69 Finance undetermined	142	25 (18)	5 (20)	20 (80)
5- 72 Credit bureau	*16*	*1 (7)*	*1 (100)*	
5- 72 Credit bureau	16	1 (7)	1 (100)	

Table 10-1
(continued)

K. Transport/tourism	*739*	*135 (18)*	*12 (9)*	*123 (91)*
K. Transport/tourism	739	132 (18)	10 (8)	122 (92)
7- 40 Transport	*63*	*26 (41)*	*3 (12)*	*23 (88)*
7- 40 Transport	63	25 (40)	2 (8)	23 (92)
7- 45 Air transport	*35*	*13 (37)*	*1 (8)*	*12 (92)*
7- 45 Air transport	35	13 (37)	1 (8)	12 (92)
7- 47 Travel agency	*67*	*13 (19)*	*4 (31)*	*9 (69)*
7- 47 Travel agency	67	13 (19)	4 (31)	9 (69)
7- 70 Hotel/tourism	*574*	*81 (14)*	*4 (5)*	*77 (95)*
7- 70 Hotel/tourism	574	79 (14)	3 (4)	76 (96)
7- 99 Undetermined		*2 (und)*		*2 (100)*
7- 99 Undetermined		2 (und)		2 (100)

L. Computer services	*153*	*35 (23)*	*13 (37)*	*22 (63)*
L. Computer services	153	33 (22)	12 (36)	21 (64)
8- 75 Computer services	*153*	*35 (23)*	*13 (37)*	*22 (63)*
8- 75 Computer services	153	33 (22)	12 (36)	21 (64)

M. Professionals	*131*	*37 (28)*	*14 (38)*	*23 (62)*
M. Professionals	131	37 (28)	14 (38)	23 (62)
8- 88 Accounting	*70*	*16 (23)*	*7 (44)*	*9 (56)*
8- 88 Accounting	70	16 (23)	7 (44)	9 (56)
8- 89 Professionals	*61*	*21 (34)*	*7 (33)*	*14 (67)*
8- 89 Professionals	61	21 (34)	7 (33)	14 (67)

N. Miscellaneous services	*234*	*41 (18)*	*10 (24)*	*31 (76)*
N. Miscellaneous services	234	40 (16)	10 (25)	30 (75)
8- 71 Advertising	*50*	*10 (20)*	*3 (30)*	*7 (70)*
8- 71 Advertising	50	9 (18)	3 (33)	6 (67)
8- 73 Mailing, Marketing	*14*	*4 (29)*	*1 (25)*	*3 (75)*
8- 73 Mailing, Marketing	14	4 (29)	1 (25)	3 (75)
8- 74 Employment	*55*	*7 (13)*	*4 (57)*	*3 (43)*
8- 74 Employment	55	7 (13)	4 (57)	3 (43)
8- 76 Security	*115*	*18 (16)*	*1 (6)*	*17 (94)*
8- 76 Security	115	18 (16)	1 (6)	17 (94)
8- 77 Collections	*10*	*2 (20)*	*1 (50)*	*1 (50)*
8- 77 Collections	10	2 (20)	1 (50)	1 (50)

Table 10-1 (continued)

0. Other	*1*	*23 (und)*	*8 (35)*	*15 (65)*
0. Other	1	21 (und)	7 (33)	14 (67)
0- 99 Undetermined (residual)		*23 (und)*	*8 (35)*	*15 (65)*
0- 99 Undetermined (residual)		21 (und)	7 (33)	14 (67)

Table 10-2
Rates of response by public sector subsector

Sector	Popul.	Resp. (%)	"Yes" (%/R)	"No" (%/R)
PUBLIC SECTOR	2211	1099 (50)	219 (20)	880 (80)
P. Education	*586*	*309 (53)*	*78 (25)*	*231 (75)*
P. Education	586	302 (52)	73 (24)	229 (76)
1- 82 Education	*586*	*309 (53)*	*78 (25)*	*231 (75)*
1- 82 Education	586	302 (52)	73 (24)	229 (76)
Q. Municipal	*297*	*161 (54)*	*10 (6)*	*151 (94)*
Q. Municipal	297	156 (53)	10 (6)	146 (94)
2- 93 Municipality	*297*	*138 (46)*	*9 (7)*	*129 (93)*
2- 93 Municipality	297	133 (45)	9 (7)	124 (93)
2- 97 Mun organization		*23 (und)*	*1 (4)*	*22 (96)*
2- 97 Mun organization		23 (und)	1 (4)	22 (96)
R. Health/social services	*1037*	*442 (43)*	*88 (20)*	*354 (80)*
R. Health/social services	1037	437 (42)	87 (20)	350 (80)
3- 80 Health	*744*	*290 (39)*	*74 (26)*	*216 (74)*
3- 80 Health	744	288 (37)	73 (25)	215 (75)
3- 83 Social services	*293*	*55 (19)*	*6 (11)*	*49 (89)*
3- 83 Social services	293	52 (18)	6 (12)	46 (90)
3- 84 Health/social services		*96 (und)*	*10 (19)*	*86 (90)*
3- 84 Health/social services		96 (und)	10 (19)	86 (90)
S. Government	*292*	*187 (64)*	*43 (23)*	*144 (77)*
S. Government	292	180 (62)	41 (23)	139 (77)
4- 91 Federal Department	*23*	*19 (83)*	*6 (32)*	*13 (68)*
4- 91 Federal Department	23	18 (78)	6 (33)	12 (67)
4- 92 Provincial Department	*216*	*112 (52)*	*22 (20)*	*90 (80)*
4- 92 Provincial Department	216	108 (50)	21 (19)	87 (81)

Table 10-2
(continued)

5- 95 Federal Organization	*11*	*16 (145)*	*6 (38)*	*10 (62)*
5- 95 Federal Organization	11	15 (136)	5 (33)	10 (67)
5- 96 Provincial Organization	*41*	*26 (63)*	*5 (19)*	*21 (81)*
5- 96 Provincial Organization	41	25 (61)	5 (20)	20 (80)
5- 99 Undetermined		*12 (und)*	*2 (17)*	*10 (83)*
5- 99 Undetermined		12 (und)	2 (17)	10 (83)

10.2 *Interpretation of rates of response*

To facilitate the understanding of these large tables, we note that our final classification does not correspond in all respects to the categories of the population. Some categories have been merged; for example, trust companies with banks. As a result, there are some empty boxes in the population which are completed in the response columns. There is one apparent anomaly: a larger number of federal organizations responded to us than the number to which we had sent the questionnaire. The reason for this was that some departments must have sent copies of the questionnaire to organizations that were more likely to respond because of the division of administrative tasks. Alternatively, some departments may have described themselves as "organization - other" without providing the information needed to identify them as departments. We put the few "Undetermined" cases from the public sector into the "Organizations" category (5) found within the "Government" group.

With respect to the composition of our sector groups, it is important to note the following comments in interpreting the rate of response:

1. In all, 47% of insurers (out of 148 possibles) responded, while the response rate among insurance agents was only 11% (out of 102 agents contacted). We might say from these figures that because the response rate among insurers is clearly one of the best in the private sector, that sector clearly took this study most seriously.
2. In business and industry, the general response rate was 23%. The response rates in the large subsectors comprising retail (N=87) and manufacturing (N=275) were only 21% and 20% respectively, construction only 17% and wholesale only 16%. The honour went to primary industry with a response rate of 30%.
3. The response rate for communications firms was 36%, counting "lates". The lower rate of response by publishers and printers (25%) brought the group down to 31%, amounting to 29% of the processed responses.
4. The general response rate of 15% in the sensitive area of financial services must be clarified. First, multiservice firms were placed in

category 69: "Undetermined" which nonetheless had 27 respondents (32% of the respondents in the sector). We would have assigned these firms to more specific subsectors if we had the information to do so. The diversification of services offered by financial institutions under provincial jurisdiction was a major obstacle here, with the result that this group covers more and more multiservice firms. Thus, it will be increasingly difficult to break it down into clearly defined subgroups by activity, except, naturally, for banks, which are under federal jurisdiction. The responses to the question on jurisdiction (question 1e of the questionnaire) show 4 or 5 "yes" replies and 17 or 18 "no" from the chartered and commercial banks, for a total of 21 to 23 respondents. The variation is owing to two respondents stating they came under both federal and provincial jurisdiction.

In the same vein, it should be noted that 17 banks and other deposit institutions, such as caisses populaires and credit unions (22%), responded. The population also included trust companies, three of which responded. The combined response rate for deposit institutions and trust companies (treated in our population as being category 60 of the SIC) would then increase to 26%, three percentage points higher than the average for the private sector. The other identifiable subsectors provided us with low response rates: only 8% for real estate agents (of which 215 were contacted) only 7% for the 16 credit bureaus (or one out of 16) and 2% for finance companies (or two out of a population of 95). Securities brokers had the distinction of giving us a nil response rate. It should be noted, however, that if we group real estate operators, promoters and investors together with real estate agents (as they were in our population), we obtain 29 responses out of 215 contacts or a rate of 13% for the "real estate subsector".

5. The "Transport/tourism" group is weighted down by the overwhelming number of hotels, only 14% out of 574 of which responded (82 respondents, nonetheless). Travel agencies contributed at a rate of only 18% while transporters were higher on the ladder, 34% for air transporters and 41% for other transporters, both of which are very acceptable rates in the private sector.

6. The miscellaneous services population included 234 firms, almost half of which (115) were in security services, the same proportion of which responded as did the group as a whole (only 16%). In the other subsectors, we found variations on low numbers: mailing and direct marketing with a 29% response rate (four respondents out of 14), collections 20% (2 out of 10), and advertising 20% (10 out of 50), while only 13% of personnel employment agencies (7 out of 55) responded.

7. We had in our population only one international organization with its head office in Canada. This organization did not return our ques-

tionnaire, but sent us a letter explaining that as an organization composed of several distinct entities it did not itself engage in transborder data flows. We therefore classified this international organization in the "Other" category of the private sector, a category for which we have no results.

8. In the public sector, there are enormous differences. In the health and social services field, 39% of health organizations (primarily hospitals) responded, while only 19% of social service organizations (excluding health) did so. It should be noted that, among social service organizations, there were many retirement homes, some of which were in the private sector where the rates of response are only half the public sector rates. In addition, many of the respondents were also care-giving institutions and, so, were classified according to the information we had in the "Health/social services" subsector. Here, we combined those that we could not divide between the two others. As a result, the rate of response in the "Social services" subsector might well be as high as that of the "Health" sector.

9. The rate of response was highest in the "Government" group. However, the response was unequally distributed. Federal departments and organizations got the highest score, with 35 responses for 34 contacts. The anomaly can be explained by multiple responses from certain organizations and by the distribution of the questionnaire by some departments to organizations under their jurisdiction. On the provincial side, we obtained 138 responses from 257 contacts, a response rate of 54%, which is four percentage points higher than the public sector average.

To close our comments, we should note that because we had a dozen organizations in the public sector that we were not able to classify with certainty in any of our categories, we arbitrarily included them under the heading "Other organizations". If we exclude these from the "Government" group, the response rate for that group drops from 64% to 60%, but it still does not fall out of first place for rates of response.

To illustrate our comments on the widely varying private sector response rates, and to put them in perspective, Table 10-3 sets out a classification of the main subsectors that contained more than 50 private firms. They are listed in ascending order by rate of response. In order to be able to compare them accurately, we have grouped together the subsectors covering deposit institutions (60 and 68) and real estate (65 and 66). Because interpretation of the public sector response rates was relatively clear, we have not included them here.

Table 10-3
Rates of response by subsector

Sector	Popul.	Resp. (%)	"Yes" (%/R)	"No" (%/R)
H- 61 Other credit	95	2 (2)	0 (0)	2 (100)
E- 64 Insurance agent	102	11 (11)	2 (18)	9 (82)
H- 65 & 66 Real estate	215	29 (13)	6 (21)	23 (79)
N- 74 Employment	55	7 (13)	4 (57)	3 (43)
K- 70 Hotel/tourism	574	81 (14)	4 (6)	77 (94)
F- 50 Wholesale	58	9 (16)	3 (33)	6 (67)
N- 76 Security	115	18 (16)	1 (6)	17 (94)
K- 47 Travel agency	67	13 (19)	4 (31)	9 (69)
H- 69 Finance undetermined	142	25 (18)	5 (20)	20 (80)
N- 71 Advertising	50	10 (20)	3 (30)	7 (70)
F- 20 Manufacturing	275	56 (20)	21 (38)	35 (72)
F- 52 Retail	87	18 (21)	2 (11)	16 (89)
L- 75 Computer services	153	35 (23)	13 (37)	22 (63)
M- 88 Accounting	70	16 (23)	7 (44)	9 (56)
G- 27 Publishing	117	29 (25)	7 (24)	22 (76)
H- 60 & 68 Deposit Inst'ns	78	20 (26)	5 (25)	15 (75)
D- 86 Nonprofit assoc'ns	270	80 (30)	29 (36)	51 (64)
M- 89 Professionals	61	21 (34)	7 (33)	14 (67)
G- 48 Communications	145	52 (36)	6 (12)	46 (88)
K- 40 Transport	63	26 (41)	3 (12)	23 (88)
E- 63 Insurers	148	70 (47)	25 (32)	45 (68)

10.3 *Differences between responses received and responses processed*

To close this section, we would like to comment on the differences between the responses actually received (including "lates" and "incompletes") and the responses processed. Given the figures shown in Table 10-1, these differences are insignificant overall, rarely causing variations of more than 2% one way or the other. We will mention here those variations that exceed 2% when the unprocessed responses are added.

- In ass[illegible]s, the response rate rises three percentage points but the proportion of "yes" and "no" replies varies by only one point.
- For insurance agents, one late "yes" doubled the number of "yes" and jumped the "yes" percentage from 10% to 18% (the number of responses N rising to two from one).
- In wholesale, the "yes" replies went from 25% to 33% (but N=3 instead of two).

- In the communications group, the "yes" responses went from 13% to 16% (N=13 instead of 10), because of a 3% increase in the publishing subsectors (N=7 instead of six) and a 4% increase in the communications subsector (N=6 instead of four).
- In real estate, we received only one late "yes", representing 9%.
- In the transportation subsector, the "yes" responses went from 8% to 12% (but only from two to three in terms of N).
- In the advertising subsector, the late arrival of one "no" lowered the proportion of "yes" from 33% to 30% (but N=3).
- In federal government departments, the late arrival of one "no" raised the response rate from 78% to 83%, for a total of 19 respondents out of 23 contacts.
- In federal organizations, the late arrival of one "yes" jumped the proportion of "yes" replies from 33% to 38%, but for a small number of respondents (N=6).

To summarize: in the sector groups on the basis of which we established our statistics, and for the respondents who engaged in transborder flows, only associations and communications showed a variation of about 3% between the results processed and the responses received. However, this was for relatively low numbers (the difference being only three respondents in each case). For respondents who did not engage in transborder flows, there was no significant variation exceeding 2%, just as there was none in the overall rate of response. There is, therefore, no cause for concern about these differences and, so, for the balance of the report, we will use only the statistics taken from the tables generated from the questionnaires we processed.

In conclusion, we would note the very great diversity in response rates when considered by subsector of activity, which is our most detailed classification. No comparison is possible with earlier studies because of a lack of refinement in the analytical tools previously used, or because of the low numbers of respondents involved where there are similar categories. It is therefore an important accomplishment to have been able through this research to determine both the rates of response and whether or not there were transborder data flows. These findings were examined not only by broad categories of public or private sector, but by 15 or so large groups and also by the 47 subsectors over which our 1,763 respondents were distributed. (There was an average of 37.5 respondents per subsector, a very comfortable number for processing and statistical analysis.) It should also be noted that when we undertake our analysis of the detailed responses of the 373 respondents who do export personal data, we will base our discussion on the 13 groups (having an average of 28 respondents per group, which is statistically still a very manageable size).

PART THREE
CHARACTERISTICS OF RESPONDENTS

Explanation of the presentation and interpretation of the results

By way of introduction to the next three parts of the report, we will explain the way we intend to present and interpret the results of our study.

Generally speaking, the procedure we intend to follow is to go from the most general to the most specific. We will therefore first deal with each of the questions in our questionnaire. We will begin with general results of the survey for that question, comparing the figures for all respondents with the figures for the public sector and the private sector. We will then examine the results by group of sectors, when the numbers make such an examination reasonable.

From time to time, in order to interpret the results, we will subdivide a variable into several components or establish a specific typology for certain questions. An interpretation will follow each set of results presented. This interpretation will then be considered in light of the interpretations of the preceding questions, when possible (we cannot cross-tabulate all our data). Interpretations will be compared (for purposes of validation) with the results of earlier studies, if they exist in respect of the question under consideration. We conclude the examination of each question with a summary of the interim conclusions, which are then brought together in a general summary in the conclusion.

For ease in presenting these results, we have changed slightly the order in which the questions are set out, from the order in our questionnaire. In Part Three, we will deal with the characteristics of the respondents: whether or not they engage in transborder data flows (questions 1 and 2). Given the large numbers involved in these questions, we have subdivided the analysis of responses into three broad questions: whether there were transborder flows, the numbers of respondents, and the jurisdictions.

In Part Four, we examine the characteristics of the data flows, analyzing respectively the use of intermediaries (question 2), transferees (question 4), and purposes (question 5). We then move on to analyze the volumes and frequencies (question 3) and the nature of the data disclosed (question 7), and to consider the method of disclosure (question 8), the form of disclosure (question 9) and protections and guarantees (question 10). We close this part with a specific examination of the respondents who stated that they engaged in very large volumes of transborder data disclosures.

Part Five consists of our analysis of the destinations of flows by country (question 6) and the legislative protection that occurs in each of these countries as revealed by our survey of the literature and our inquiries to authorities and diplomatic representatives from the countries that receive significant personal data flows concerning Canadians.

Before moving on to the analysis proper, we should interject a note of caution about the interpretations that can be drawn from our results. These results were obtained on the basis of responses from a group of private firms and public organizations (the population) consisting of a large number of entities that belong to what are, in our view, the sectors of activity most likely to engage in transborder personal data flows. However, in terms of the types of questions that interest us, we did not know the structural characteristics of each of the sectors of activity that make up our population: the occurrence and structure of files and communications networks, and the occurrence of data flows. This is the major difficulty in our study; our work is exploratory. These are precisely the matters on which we sought new data or data that exist only in fragmentary form.

Because we could not know in advance the actual nature of the data we were to receive, we could not use information variables to control the composition of the sectors of activity being studied, as we explained in point 2 of Part Two. We therefore cannot, solely on the basis of the statistics compiled, make any judgment as to the representativeness of our responses in relation to the entire population surveyed or to the sectors of activity examined. In these circumstances, it did not appear useful to weight the data by sector or to conduct statistical significance tests. Generally speaking, our results might be significant overall or for the sectors in question, but we cannot demonstrate this statistically.

These factors show the crudeness of the tools that are available to examine a subject of such delicacy and complexity. However, in the circumstances and given the constraints of our study, it is possible to arrive at meaningful conclusions using other equally valid methods. First, we can look for structural consistency within our sectors, by comparing them to each other. In this way we can find similar patterns in the responses and consistencies or contrasts. We can also use ranking techniques, which show indicators that may help considerably in our explanations. Finally, we can compare our results with the results of similar studies. Knowledge of the sectors, gleaned from our survey of the literature or drawn from our own expertise, will also provide a foundation for our interpretations. This is the best that can be done given the present state of the methodology available at the international level for this kind of study, taking into account the time and budget constraints within which we had to work.

Generally speaking, we can state at the outset, having examined the responses sent to us and on the basis of the hundreds of letters and telephone calls we received after mailing out our questionnaire, that none of the sectors of activity systematically refused or declined to respond to the questionnaire.

We must admit that in some subsectors of the finance group the rate of response was very low, falling below 10% (other credit institutions: N=2; securities brokers: N=0; investment firms: N=5; trust companies: N=3). This is owing to the fact that we subdivided this group into very fine subsectors. It may also be that some of the 25 respondents classified in the "Undetermined or composite" subsector might well belong to one of our almost-empty categories. Nonetheless, the average rate of response in this group (15%) is 8 points lower than the average rate of response for the private sector (23%). This is a large difference (-35%). It raise questions about the degree of social responsibility of the firms in this sensitive sector, which should have felt strongly about this study given what we already know about their data activities.

Overall, however, we can summarize by saying that the observed rates of response do not disclose any significant bias that would prevent us from drawing valid conclusions on our sector groups. Of course, we will have to take certain precautions in interpreting the available results in some subsectors.

We must state another important reservation relating to the relative lack of knowledge of the issue on the part of some of our respondents. We were working here in a very new field that has not been studied to any great extent, and about which there is still very little awareness and practically no academic training. Moreover, little legislation has been enacted in Canada with respect to the protection of personal data (federal, Quebec and Ontario legislation still applies only to the public sector). It may well be that in other jurisdictions, as well as in the private sector, awareness of personal data protection is much less advanced than in those public organizations that must regularly satisfy legislative requirements. Moreover, where there is no one person who is responsible for personal data protection, often no one knows exactly how decentralized indexes are managed.

There is one additional major difficulty. What happens with respect to data transfer is not always easily discerned. By definition, transfers take place at the junction of several operations. Thus, there may not always be a key person in the various organizations who would be familiar with all aspects of these operations and so be the ideal respondent. In organizations where a figure has never been set on the volumes and frequencies of transborder personal data flows, it may be impossible to do so, or possible to give only a very rough approximation.

Given these circumstances, it is inevitable that some of our respondents, particularly those in categories where the volumes were low, might not have been fully aware of all the facts and of some matters raised by our questionnaire. We should not be surprised that, despite their good faith, they have not yet conceptualized their practices in terms of personal data management. We will, therefore, have to take these points into account in interpreting the responses we received, particularly when we come to assess the scope of the phenomenon.

These comments, however, do not apply to all sectors of activity. This is so particularly with those organizations that operate at the pinnacle of technological development in the area of data management. These organizations include financial institutions, air carriers and some large firms engaged in trading in information, as well as some public organizations that maintain very large indexes on individuals. These organizations have considerable expertise in the issues examined in our study, both in technical and organizational terms and in terms of awareness of the economic, social and political issues involved in their practices. The largest of them have even adopted codes of ethics or conduct to govern these practices and to reassure the general public about the principles they apply in managing their data. We cannot, therefore, suspect lack of knowledge or awareness. Where there are inconsistencies between what we know and what they have stated about their practices, there may be sectoral distortions in assessing the results of this survey.

Finally, as in any study of this nature, we have been limited by the constraints involved in writing the questionnaire. To maximize the response rate, we could not go into too many details or branch out in too many directions, thus limiting the cross-tabulation possibilities for our data. For example, we could not ask respondents to list volumes and frequencies of flows by both categories of people (clients, employees, other) and countries of destination. For purposes of quantitative interpretation, we had to amalgamate some possibilities, both in formulating the suggested responses and in coding the responses received. More detailed categories would clearly have resulted in a lower response rate and in a greater proportion of questions being unanswered.

1 The occurrence of transborder flows

In this first section, we are going to examine the extent to which there are transborder flows of data leaving Canada. The question in issue was posed in question 2 of the questionnaire, immediately following the respondent's identifying data. It read as follows:

2. In the course of your operations, do you transfer data to a foreign destination, on a regular or occasional basis, concerning persons living in Canada or Canadians living abroad (by sending such data or giving access to it)?

The response rate for this question has already been indicated in Part Two of the report, because question 2 was what we used to separate the respondents who stated that they engaged in transborder flows ("yes") from those who stated that they did not ("no"). We used this to determine, without comment, the relative "yes" and "no" rates in the various sectors, groups and subsectors. We will now return to this basic data, examining it from the most general to the most specific (i.e., as a whole, sector, group, subsector) and rank the results from the lowest "yes" rates to the highest "yes" rates.

1.1 Overall results by large sector

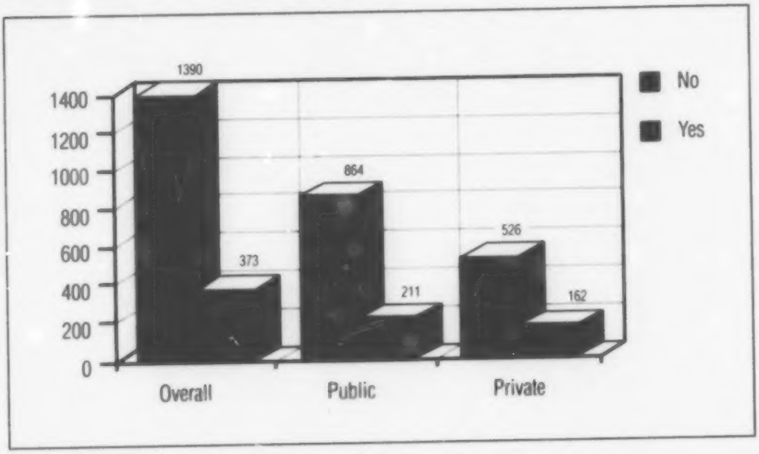
We will now present the results as a whole for our two large sectors, public and private, and analyze the data and comment. The following tables set out the results of the survey on the basis of the responses processed, in the same format as earlier (i.e., calculating, in turn, the size of the sample, the overall rate of response, the number and proportion of respondents who stated they engaged in flows, and the number and proportion of respondents who stated they did not engage in such flows).

Table 1-1
Occurrence of flows by large sector

Sector	Mailed	Responses (%)	Yes (%/R)	"No" (%/R)
OVERALL	5291	1763 (33)	373 (21)	1390 (79)
PUBLIC SECTOR	2211	1075 (49)	211 (20)	864 (80)
PRIVATE SECTOR	3080	688 (22)	162 (24)	526 (76)

These figures show that, for a third of our sample, the proportion of respondents who engage in transfers of data outside Canadian borders is in the order of 21%, with a substantial variation between the private sector with 24%, and the public sector with only 20%. These figures do not indicate the sizes of these flows, but show only that they occur within these organizations. Graphic 1-1 visually illustrates these overall results.

Graphic 1-1
Occurrence of flows by large sector



1.2 *Comparison with the results of other studies*

Overall, the figures here were a little higher than in the 1988 study on data disclosures as revealed in responses to a question about the occurrence of transborder data flows. Of 432 respondents, 67, or 15.5% of the total, reported they transferred personal data abroad. There are two possible explanations for this difference: either the incidence of transborder flows increased during the past two years, or such flows occurred at the time but our respondents were more aware of them when answering a questionnaire dealing specifically with this issue.

We can also add that several respondents reported in this study that they engaged only occasionally in personal date flows, particularly in the public sector, among educational institutions and health service institutions. Some declined to answer when this was the case, arguing that their response could skew our data because their volumes were insignificant. These respondents may simply have responded in the negative in the first study, explaining the lower positive response observed.

Of the other empirical studies relating to our topic, only the study by IBI in 1983 attempted to assess the real incidence of transborder data flows. Of the total of 380 respondents, 80% came from the Third World, only 15 being from Canada and 13 from the United States (representing only 7.6% of the 300 North American firms contacted). Of these, 80% were private firms with 56% being multinational firms. Fewer than 20% of the respondents in this 1983 study stated that they transferred personal data to another country (IBI, p. 11). We learn no more from reading this study, apart from the fact that it does indicate that our results, 21% overall and 24% in the private sector, are about the same magnitude.

In terms of comparing the public and private sectors, the only comparable figures available to us were in the 1988 GRID study. In that case, 34 private firms out of 139, or 24%, and 34 public organizations out of 293, or 12%, stated that they engaged in transborder data flows to foreign destinations. For the private sector, our data did not vary, despite the great difference in the response rate (139 usable questionnaires out of 3,169 sent, for a rate of only 4.5%). For the public sector, our results were much lower, despite, or perhaps because of, a much higher response rate (293 usable questionnaires out of 1,519 sent, for a rate of 19%).

To summarize, we found that 21% of our respondents engaged in transborder personal data flows to destinations outside Canada, with a slightly higher figure for the private sector (24%) than for the public sector (20%). These rates are comparable for the private sector to those found in two earlier studies (IBI and GRID) but substantially exceed the rate found by GRID in 1988 for the public sector.

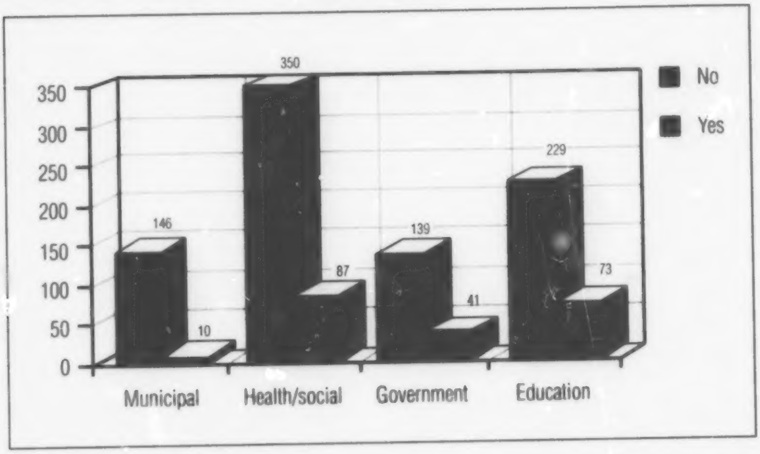
1.3 *Results for public sector groups*

We will now consider the results by group of subsectors, starting with the public sector groups. In Table 1-2 and Graphic 1-2, we ranked these figures by increasing order of positive responses to the question whether there were transborder personal data flows to destinations outside Canada.

Table 1-2
Occurrence of flows by public sector group

Public sector	Sent	Resp. (%)	"Yes" (%/R)	"No" (%/R)
PUBLIC SECTOR	2211	1075 (49)	211 (20)	864 (80)
Q. Municipal	297	156 (53)	10 (6)	146 (94)
R. Health/social	1037	437 (42)	87 (20)	350 (80)
S. Government	292	180 (62)	41 (23)	139 (77)
P. Education	586	302 (52)	73 (24)	229 (76)

Graphic 1-2
Ocurrence of flows in the public sector

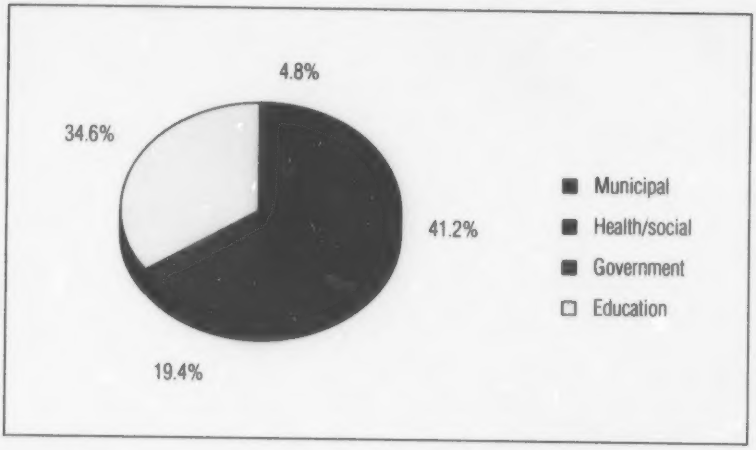


In the public sector, the fact that emerged most clearly was the low rate (6%) at which municipalities and municipal organizations engaged in international exchanges of personal data. This was expected owing to the local nature of their activities. For other groups, while their rates of response varied widely, the rates at which they engaged in transborder flows were comparable: 20% for health and social services, 23% for government departments and organizations and 24% for educational institutions. We may assume that significant differences will appear when we examine the volume and content of such exports.

It is important to note at this point that, overall, a relatively high proportion of the public and quasi-public organizations that responded to our survey (excluding municipalities) engaged in transfers of data to destinations outside the country. We might hypothesize that this phenomenon was a function of the expansion of government programs and services, the growing internationalization of relations among countries and more frequent travel by people to destinations outside the country (receiving health care abroad, pursuing education abroad, and so on).

To close on this point, Graphic 1-3 shows each of our groups as a proportion of public sector exporters as a whole.

Graphic 1-3
Distribution of exporters in the public sector



1.4 Results for private sector groups

Table 1-3 shows the response rate for groups in the private sector, by increasing order, and whether they engage in personal data exports. Graphic 1-4 illustrates these results.

Table 1-3
Occurrence of flows by private sector group

Private sector	Sent	Resp. (%)	"Yes" (%/R)	"No" (%/R)
PRIVATE SECTOR	3080	684 (22)	162 (24)	526 (76)
K. Transport-tourism	739	132 (18)	10 (8)	122 (92)
G. Communications	262	77 (29)	10 (13)	67 (87)
H. Finance	555	81 (15)	17 (21)	64 (79)
N. Misc Services	234	40 (16)	10 (25)	30 (75)
F. Business/Industry	485	110 (23)	31 (27)	79 (73)
E. Insurance	250	83 (33)	25 (30)	58 (70)
O. Other	1	21 (und)	7 (33)	14 (57)
D. Associations	270	74 (27)	26 (35)	48 (65)
L. Computer Services	153	33 (22)	12 (36)	21 (64)
M. Professionals	131	37 (38)	14 (38)	23 (62)

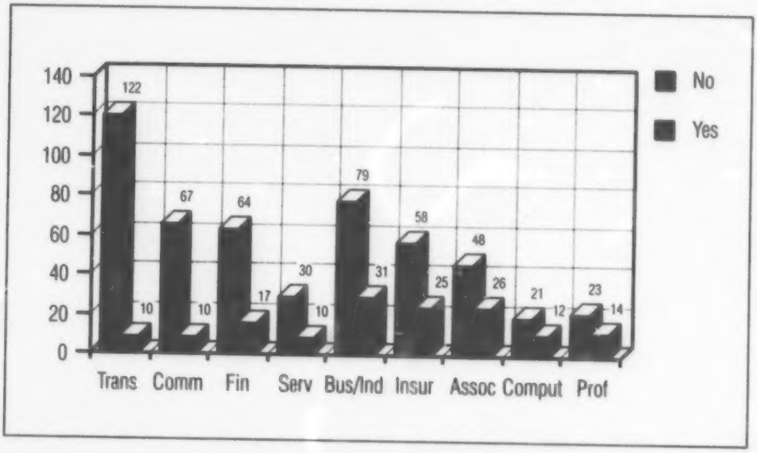
Within the private sector, there are relatively few transborder data flows among respondents in "Transportation and tourism" (8%) and "Communications" (13%), areas where we would have expected much greater involvement in international data flows. These low scores may be owing to the fact that hotels, which form a majority of the respondents in our "Transportation and tourism" group, send very little personal data to destinations outside the country (we will examine this case later). In the communications group, it is possible that personal data were circulated primarily by press agencies, of which there were relatively few in Canada, and even fewer of which were international in scope. We will return to this question in examining the subsectors, to discover whether there are contrasts to explain the lack of flows.

We have already examined the low rates of response in the finance group. Among those who responded, the proportion that engaged in personal data exports (21%) was also below the private sector average (24%). This figure is surprising, given the size of personal data bases in this sector. GRID's initial research confirmed the extent to which computerized networks and data bases had been developed in this sector by 1986. In the financial sector, which accounted for 34% of the private sector respondents in the 1988 GRID survey, and included insurers, 40% of respondents transmitted personal data abroad. However, if we exclude insurers from these figures, we are left with the banks, where only two out of nine (22%) stated that they engaged in such transfers. This corresponds to the average observed in the present study, but we must refine our analysis by examining the distribution of these responses among the subsectors.

We have no particular comments to make with respect to the scores of the "Miscellaneous services" (25%) and "Business and industry" (27%) groups, except to note that we did not expect such high figures for business and, particularly, for industry where the primary activity was not processing personal data. Because of the very diversity of these groups, we will reserve our interpretation until we examine the results by subsector and by type of data exported. For the "Other" category, it is unfortunate that we did not receive sufficient information to be able to put the seven respondents in question into one of the other sectors. This helped bring down the averages in the other groups.

The export rate in the insurance group was 30%, lower than the 64% found in the 1988 study (18 out of 28 insurers) but a good indication of the significance of flows in this sector. We could say much the same thing with respect to associations where the "yes" rate was 35%. This sector scored on the order of 71% in 1988, but for fewer cases (10 respondents out of 14).

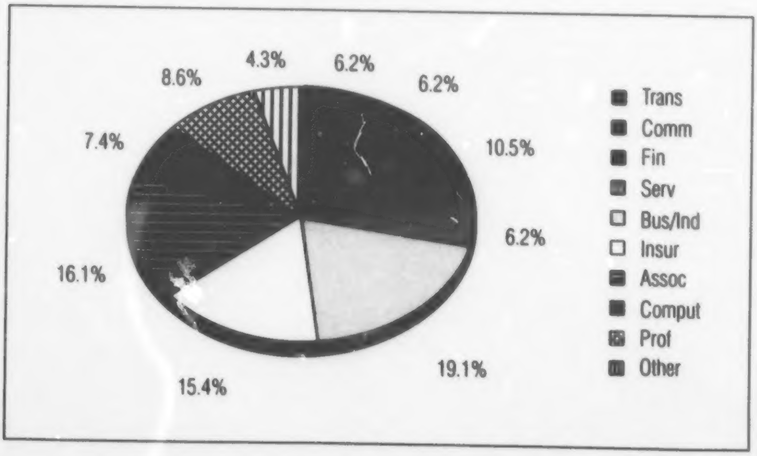
Graphic 1-4
Occurrence of flows in the private sector



At the top of the list we have computer services and professionals (accountants, consulting engineers and so on) with rates of 36% and 38%. These rates should not be surprising in the case of computer services firms, because they process and circulate data. Large volumes of personal data flows are also reported by professionals offering specialized services. It would be interesting to investigate this phenomenon further by conducting consultations and interviews that would provide us with the reasoned interpretations of the participants.

To conclude, Graphic 1-5 shows each of the groups as a proportion of private sector exporters as a whole.

Graphic 1-5
Distribution of private sector exporters



1.5 *Results by public sector subsectors*

We will refine our analysis of the occurrence of transborder data flows by examining the subsectors by increasing order of positive responses and by groups of sectors as set out in the previous paragraph. We will deal first with the public sector and secondly with the private sector. We will then rank these subsectors again, by increasing order of involvement in data flows, regardless of group, to determine specific details. For the public sector, Table 1-4 presents the results by increasing order for groups that export personal data.

Table 1-4
Occurrence of flows by public sector subsector

Public Sector	Sent	Resp. (%)	"Yes" (%/R)	"No" (%/R)
Q. Municipal	297	156 (53)	10 (6)	146 (94)
2- 93 Municipality	297	133 (45)	9 (7)	124 (93)
2- 97 Mun organization		23 (und)	1 (4)	22 (96)
R. Health/soc serv	1037	437 (42)	87 (20)	350 (80)
3- 80 Health	744	288 (37)	73 (25)	215 (75)
3- 83 Social services	293	52 (18)	6 (12)	46 (90)
3- 84 Health-soc serv		96 (und)	10 (19)	86 (90)
S. Government	292	180 (62)	41 (23)	139 (77)
4- 91 Fed Department	23	18 (78)	6 (33)	12 (67)
4- 92 Prov Department	216	108 (50)	21 (19)	87 (81)
5- 95 Fed Organization	11	15 (136)	5 (33)	10 (67)
5- 96 Prov Organization	41	25 (61)	5 (20)	20 (80)
5- 99 Undetermined		12 (und)	2 (17)	10 (83)
P. Education	586	302 (52)	73 (24)	229 (76)
1- 82 Education	586	302 (52)	73 (24)	229 (76)

Remarkably, municipalities and, particularly, municipal organizations, contribute a significant amount, or represent a significant proportion of, personal data exports. The differences by subsector are greater in the "Health and social services" group, where 25% of health institutions (essentially hospitals) engage such activities, while only 10% to 12% of the others do so. Because education is dealt with as a compact whole for purposes of analysis, our earlier comments on the education group apply to it as a whole.

The more diversified "Government" group remains. Here, there are two potential divisions. The distinction between departments (21%) and organizations (25%) resulted in no appreciable difference. Jurisdiction is a more significant criterion: 33% of federal departments and organizations export personal data, while only 19% to 20% of provincial departments and organizations do so. This may be because of the different missions of these two levels of government or because of greater awareness on the part of federal organizations, which are all subject to the provisions of personal data protection legislation. Only Quebec and Ontario have such legislation at this time. Or, the difference may be owing to the effect of size, reflecting the greater coverage that federal organizations provided us or their greater interest in and sensitivity to this study, which was conducted on behalf of the federal government. These are all plausible explanations.

1.6 *Results by private sector subsectors*

Table 1-5 presents the results for the private sector, by increasing order, for groups that export personal data.

Table 1-5
Occurrence of flows by private sector subsector

Private Sector	Sent	Resp. (%)	"Yes" (%/R)	"No" (%/R)
K. TRANSPORT/TOURISM	739	132 (18)	10 (8)	122 (92)
7- 40 Transportation	63	25 (40)	2 (8)	23 (92)
7- 45 Air transport	35	13 (37)	1 (8)	12 (92)
7- 47 Travel agency	67	13 (19)	4 (31)	9 (69)
7- 70 Hotel/tourism	574	79 (14)	3 (4)	76 (96)
7- 99 Undetermined		2 (und)		2 (100)
G. COMMUNICATIONS	262	77 (29)	10 (13)	67 (87)
4- 27 Publishing	117	28 (24)	6 (21)	22 (79)
4- 48 Communications	145	49 (34)	4 (8)	45 (92)
H. FINANCE	555	81 (15)	17 (21)	64 (79)
5- 60 Banking	78	17 (22)	5 (29)	12 (71)
5 -61 Other credit	95	2 (2)		2 (100)
5- 62 Securities	9	0 (0)		
5- 65 Real estate		10 (und)		10 (100)
5- 66 Real estate agent	215	18 (8)	5 (28)	13 (72)
5- 67 Investment company		5 (und)	1 (20)	4 (80)
5- 68 Trust co (see 60)		3 (und)		3 (100)
5- 69 Fin undetermined 142		25 (18)	5 (20)	20 (80)
5- 72 Credit bureau	16	1 (7)	1 (100)	

Table 1-5
(continued)

N. MISC SERVICES	234	40 (16)	10 (25)	30 (75)
8- 71 Advertising	50	9 (18)	3 (33)	6 (67)
8- 73 Mailing, Mkting	14	4 (29)	1 (25)	3 (75)
8- 74 Employment	55	7 (13)	4 (57)	3 (43)
8- 76 Security	115	18 (16)	1 (6)	17 (94)
8- 77 Collections	10	2 (20)	1 (50)	1 (50)
F. BUSINESS/INDUSTRY	485	110 (23)	31 (27)	79 (73)
3- 50 Wholesale	58	8 (14)	2 (25)	6 (75)
3- 52 Retail	87	18 (21)	2 (11)	16 (89)
3- 59 Und Bus/Ind		3 (und)		3 (100)
6- 10 Primary	47	14 (30)	6 (43)	8 (57)
6- 15 Construction	18	3 (17)		3 (100)
6- 20 Manufacturer	275	55 (20)	20 (36)	35 (64)
6- 49 Public services		2 (und)		2 (100)
E. INSURANCE	250	83 (33)	25 (30)	58 (70)
2- 63 Insurer	148	69 (47)	24 (32)	45 (68)
2- 64 Insurance agent	102	10 (10)	1 (10)	9 (90)
2- 99 Undetermined		4 (und)		4 (100)
D. ASSOCIATIONS	270	80 (30)	29 (36)	51 (64)
L. COMPUTER SERVICES	153	33 (22)	12 (36)	21 (64)
M. PROFESSIONALS	131	37 (28)	14 (38)	23 (62)
8- 88 Accounting	70	16 (23)	7 (44)	9 (56)
8- 89 Professionals	61	21 (34)	7 (33)	14 (67)

1. With respect to the transportation and tourism group, transborder flows were effected mainly by travel agencies (31% of respondents). However, we are dealing here with small numbers (4 respondents out of 13). Only 8% of each of transporters and, in particular of air carriers, reported that they engaged in such flows. There was no "late" response to raise this low score. Among hotels, there was little activity in this area. If we assume that travel agencies conduct a portion of their business on site with wholesalers operating in Canada, it is difficult to see how air transportation companies could engage in so few transborder data flows, unless only the local carriers responded to us. In fact, any international passenger transportation involves transborder data flows.

The same is true, but to a lesser extent, for transportation firms. A larger proportion of these firms engages only in local or interprovincial data flows. However, we were surprised there were so few transborder personal data flows. We might assume that large transport companies ship all kinds of material within Canada, but they must also send personal data to recipients abroad. In the hotel industry, it is plausible that only the large multinational chains have an international reservation system and that others, not affiliated with such organizations, have no occasion to export personal data.

2. We now come to the field of communications. Here, the response rate for publishers and printers (excluding electronic publishers in radio, television and cable TV, which we classified in the communications subsector, and computer or telematics publishers, which we classified in the computer services subsector) was 21%, substantially the same as the average for the private sector. Surprisingly, the rate of response of the communications subsector, which is composed mainly of radio, television and cable firms, and telephone services, was a respectable 34%, (N=49 out of 145), with only 4 out of 49 respondents reporting that they export personal data. Do these firms produce no exportable personal data? Do they rely exclusively on press agencies (which were included in our population in the same category) to disseminate such information? Apparently, telephone firms believe they do not own the data passing through their networks to points outside the country. If so, this would explain the few "yes" responses from this group.

3. "Finance" also ranks below the private sector average for involvement in transborder personal data flows. However, there were significant variations here, not only in the rates of response but in the proportion of firms that exported data. Here, 29% of the banks and 28% of real estate agents exported data, a higher rate than the private sector average. Nonetheless, in our view, the figure is low for banks. It should be noted, however, that this subsector included deposit institutions that may transmit their funds and personal data through banks. On the other hand, the rate is high for real estate agents. (Real estate is, by definition, local but it includes an increasingly large international investment sector.)

   We found that only one firm in each of the two subsectors consisting of investment companies and credit bureaus (only one of which responded) reported that they exported personal data. We assume that transborder personal data flows are common practice in these subsectors, particularly in the latter. The score for personal data exports in the other subsectors (trusts, property management, securities brokers, credit institutions) was nil. The rates of response were so low that we must report they provided us with practically no usable information to assess data flows in this field. However, in 1988 we received three positive responses from trust companies, indicating exports of personal data abroad, and two positive responses from loan companies. To summarize, we can confirm that transborder personal data flows indeed occur in banks and similar institutions as well as in real estate. Confirmation from the rest of the firms in this area was not forthcoming.

4. In the case of miscellaneous services, diversity is the rule. We first eliminated from our examination collections and mailing and marketing, sectors where the sample was small because of the size of the firms and where, in each case, we had only one positive. The security subsector (detective and security agencies) provided us with little more, despite the number of firms in the sample (115 contacted). We were left with advertising agencies, where three out of nine (33%) did export personal data, and personnel employment agencies, where four out of seven (57%) did so, out of populations of 50 and 55 firms respectively. These figures are interesting in that they show the importance of transborder personal data flows relating to employment (for personnel employment agencies) and advertising, which is similar to marketing. (Because the borders between these fields are not strictly defined, the sector also includes advertising by mail and other media.) On the basis of these results, we might conclude that advertising is becoming increasingly dependent on the use of personal data.

5. We now come to the business and industry sectors. We note that we contacted some 500 of the largest Canadian firms. With an acceptable response rate, 27% of these firms, which we did not particularly target, reported they exported personal data. This is somewhat surprising. Later in our analysis, we will see what is involved in these exports. For the moment, we note that 25% of respondents in wholesale business reported they exported personal data (but N=2 out of 8), as did 36% in the manufacturing sector (N=20 out of 55) and 43% in the primary sector (mines and forests, but N=6 out of 14). The performance of the manufacturing sector is remarkable here, given the numbers involved, indicating that the various components of this subsector merit closer observation.

6. The rate of data exports among insurers (30%) is considerably higher than the average, and if we exclude insurance agents (only one of which reported flows) and "Undetermineds" (which reported none) the rate for insurance companies rises to 32%, slightly higher than for banks and real estate agents.

7. Nonprofit associations with a "yes" rate of 35% were grouped into one multi-category so that the comments made earlier in point 1.2 about this group apply here as a whole. The same is true for the computer services sector, with a score of 36%. Finally, the professionals group takes first place with 38% exporting personal data. This group includes accountants, who lead the group with an export rate of 44%, a figure for which we do not have a ready explanation, given the diversity of this subsector.

1.7 *Significant variations among subsectors*

To summarize, by examining the rates of involvement in transborder data flows by subsector, we have been able to draw finer distinctions in the analysis we propose to conduct of the large groups with which the analysis will deal. The subsectors that must be seen as more important than the average for their groups are as follows (we indicate the variation from the group average in parentheses):

- personnel employment agencies in the miscellaneous services group (+32% with N=4);
- travel agencies in the transportation group (+23%, but N=4);
- the primary sector (+16%, but N=6) and manufacturing sector (+9%, with N=20) in the business and industry group;
- federal departments and organizations in the government field (+10% each, with N=11 overall);
- publishers in the communications field (=8%, but N=6);
- banks and similar organizations and real estate agents in the finance group (+8% and +7% respectively, but N=5 for each of these subsectors);
- advertising agencies in miscellaneous services (+8%, with N=3);
- accounting in professional services (+6%, with N=7);
- hospitals (+5%, but N=73).

The subsectors that show substantial positive variations from the average for their groups are shown in the following table, by increasing order of variation from the average:

Table 1-6
Occurrence of flows by subsector

Sector	Sent	Resp. (%)	"Yes" (%/R)	Variation from average
R- 80 Health	744	288 (37)	73 (25)	(+ 5)
M- 88 Accounting	70	16 (23)	7 (44)	(+ 6)
H- 66 Real Estate Agent	215	18 (23)	5 (28)	(+ 7)
G- 27 Publishing	117	28 (24)	6 (21)	(+ 8)
H- 60 Bank	78	17 (22)	5 (29)	(+ 8)
N- 71 Advertising	50	9 (18)	3 (33)	(+ 8)
F- 20 Manufacturing	275	55 (20)	20 (36)	(+ 9)
S- 91 Fed department	23	18 (78)	6 (33)	(+10)
S- 95 Fed organization	11	15 (136)	5 (33)	(+10)
F- 10 Primary	47	14 (30)	6 (43)	(+16)
K- 47 Travel agency	67	13 (19)	4 (31)	(+23)
N- 74 Employment	55	7 (13)	4 (57)	(+32)

The following table ranks the subsectors by increasing order of involvement in personal data exports and shows the variation from the group averages; providing an even better illustration of certain contrasts. We have deliberately removed categories with one or two cases from this table.

Table 1-7
Occurrence of flows by subsector

Sector	Sent	Resp. (%)	"Yes" (%/R)	Variation from average
K- 70 Hotel-tourism	574	79 (14)	3 (4)	(- 4)
Q- 93 Municipality	397	133 (45)	9 (7)	(+ 1)
G- 48 Communications	145	49 (34)	4 (8)	(- 5)
R- 84 Health/Soc serv		96 (und)	10 (10)	(-10)
R- 83 Social services	293	52 (18)	6 (12)	(- 8)
S- 92 Prov department	216	108 (50)	21 (19)	(- 4)
S- 96 Prov organization	41	25 (61)	5 (20)	(- 3)
H- 69 Finance (und)	142	25 (18)	5 (20)	(- 1)
G- 27 Publishing	117	28 (24)	6 (21)	(+ 8)
P- 82 Education	586	302 (52)	73 (24)	(idem)
R- 80 Health services	744	288 (37)	73 (25)	(+ 5)
H- 66 Real estate agent	215	18 (8)	5 (28)	(+ 7)
H- 60 Bank	78	17 (22)	5 (29)	(+ 8)
K- 47 Travel agency	67	13 (19)	4 (31)	(+23)
E- 63 Insurer	148	69 (47)	24 (32)	(+ 2)
N- 71 Advertising	50	9 (18)	3 (33)	(+ 8)
M- 89 Misc professional	61	21 (34)	7 (33)	(- 5)
S- 91 Fed department	23	18 (78)	6 (33)	(+10)
S- 95 Fed organization	11	15 (136)	5 (33)	(+10)
D- 86 NP Association	270	74 (27)	26 (35)	(idem)
F- 20 Manufacturing	275	55 (20)	20 (36)	(+ 9)
L- 75 Computer Services	153	33 (22)	12 (36)	(idem)
F- 10 Primary	47	14 (30)	6 (43)	(+16)
M- 88 Accounting	70	16 (23)	7 (44)	(+ 6)
N- 74 Employment	55	7 (57)	4 (57)	(+32)

1.8 *Summary and conclusions*

The principal findings of the 1,762 responses processed are that 21% of respondents engaged in personal data exports. There was a substantial difference between the public sector (only 20% of which export) and the private sector (24%). This confirms the trend found in the 1985 GRID study of private personal data bases in Quebec. With respect to the accumulation and distribution of personal data, the growth of data bases and in communications networks in the private sector has made it as least as important, if not more so, than the public sector. Does the relatively greater involvement of the private sector in exporting data reflect this general trend, or is it the result of specialization by private firms in this kind of transfer? This is an important question because only the public sector is affected by Canadian personal data protection legislation, enacted by the federal and Quebec governments in 1982, and by Ontario in 1987. We will later identify certain factors that will allow us to further refine this hypothesis.

Our analysis of the groups of subsectors illustrates the great diversity that exists in transborder personal data flows. We expected that certain groups, which had been more specifically targeted by earlier studies (such as insurers, or even associations), would show greater activity, as was confirmed by scores of 30% and 35% respectively. However, we were surprised to find that other groups, which at first glance appeared to be very involved in personal data exports (such as transportation and tourism, communications and finance), had scores below the private sector average (8%, 13% and 21%, respectively). On the other hand, the business and industry group scored well at 27%, contrary to our expectations. Computer services and professional firms had the best performance, as it were, with rates of 36% and 38%. In the public sector, the results were close to the sector average (20%) except for municipalities, which are much less involved in such exchanges (only 6%). In terms of personal data exports, we found great diversity in the private sector and relative uniformity in the public sector.

Examination of the subsectors that make up our groups provided us with details on the distinctions that must be made in considering the foregoing comments. This examination also highlighted certain subsectors of activity where results were markedly higher than the average for their group: personnel employment agencies, travel agencies, primary and manufacturing industries, publishers, banks, real estate agents and advertising agencies, as well as federal departments and organizations that are particularly active in terms of the public sector. Conversely, we also found incongruities in the other direction. It is difficult to believe that so few personal data are exported in such subsectors as transporters, air carriers, electronic and telephone communications firms, credit institutions, investment companies, credit bureaus, securities brokers and security services.

We will now expand on these findings, and indicate their finer distinctions, by more closely examining the size of these flows, their destination and nature, the methods and forms of transmission and the protections and guarantees to which they are subject.

2 Number of clients

In the first question asking for their identifying data, we asked all respondents to tell us the size of their firm or organization in terms of numbers of clients and people employed. The question was: "What is your approximate number of clients?" (or persons under your administration). Question 1d) was: "What is your approximate number of employees?" The question on number of clients serves to introduce the third question on volume of flows because data exports involve clients as a whole. With respect to the number of employees, we established a threshold of 100 employees for our population of public organizations; of 50 employees for private firms in the "target sectors"; and as many employees as possible for the 750 "residual" firms (mainly the manufacturing, business and finance sectors). We should therefore expect to obtain corresponding figures here, subject to restructuring, fluctuations in numbers of employees, and so on.

We will therefore examine the results of the responses to these two questions to try to determine, specifically, the extent to which the size of the respondents may be a factor in explaining the variations found in whether or not there are transborder personal data flows.

2.1 Results overall and for large sectors

Table 2-1 sets out the responses to the question dealing with numbers of clients, overall and for the public and private sectors. In order to facilitate comparison and to assess the value of each variable in explaining the results, the "yes" (exporters) responses are indicated in boldface followed by the "no" (non-exporters) responses in normal type. In addition, we calculated the average for each category out of the total of 1,763 respondents. For comparative purposes, the values are given in percentages; however, as the non-responses are not counted (they amounted to about 3% to 4%), the percentages do not always add up to 100%.

Table 2-1
Number of clients by large sector

Sector		**-10,000 (%)**	**10-50,000 (%)**	**50-100,000 (%)**	**100,000 (%)**
OVERALL	yes:	**38**	**19**	**12**	**28**
	no:	50	22	8	16
	average:	47	22	9	19
PUBLIC SECTOR	yes:	**32**	**21**	**16**	**29**
	no:	50	24	8	14
	average:	46	24	10	17
PRIVATE SECTOR	yes:	**46**	**24**	**10**	**17**
	no:	50	19	8	20
	average:	49	19	7	21

In the following analyses, we designated numbers of clients as follows: fewer than 10,000 people as "small"; 10,000 to 50,000 people as "medium"; 50,000 to 100,000 people as "large"; more than 100,000 people as "very large". We did the same to establish four size categories for number of employees and volume of exports. However, because of the lack of existing data in other studies, we cannot compare our data and thus propose further interpretations that would confirm or invalidate our conclusions.

1. Because of the large number of "no" responses (80% of all responses), the average for respondents is very close to the average for the "no" responses. The greatest variation was no more than 6% and most of the variations were between 2% and 4%. We can therefore concentrate our analysis on comparing the "yes" and "no" responses.

2. If we consider the entire group of respondents who export personal data, we find that most had fewer than 50,000 clients (57%). The greatest proportion, 38%, had fewer than 10,000 clients, while only 28% of respondents had more than 100,000 clients, a number indicating their importance in economic and social terms.

   On the other hand, when we consider the figures on the "no" side, we find that the effect of the number of clients is greater. Here, 50% of respondents had fewer than 10,000 clients, while only 16% had more than 100,000. At both ends of the scale there was a difference of 12 points. If we compare percentages between the groups, we find that a personal data exporter had a 24% lower chance of being in the category of firms with fewer than 10,000 clients than did a respondent reporting no flows, while it had a 75% greater chance of being in the category of organizations with more than 100,000 clients.

Thus, we find that the number of clients is a variable that may be used to explain whether or not there were transborder personal data flows among respondents making up a third of our population: the more clients a respondent had, the greater the chance that the respondent was an exporter of personal data.

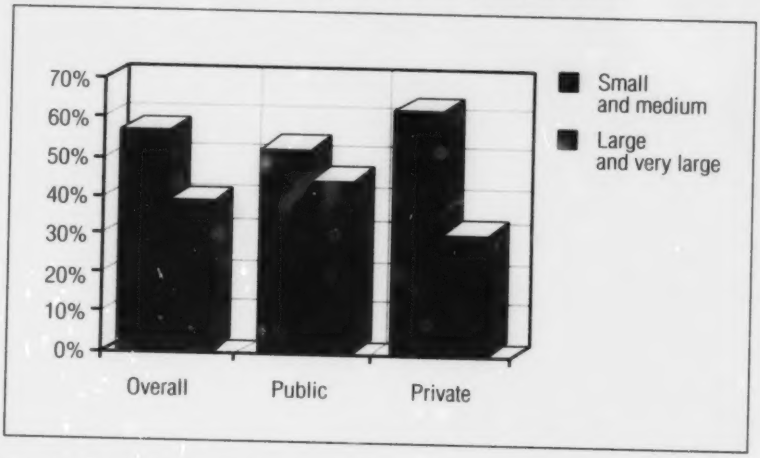
3. Public sector figures reflect the same situation, but with larger variations. In the category of fewer than 10,000 clients (or persons under the administration of the organization), we found only 32% of data exporters but 50% of the non-exporters, a difference of 18 points this time. On the other hand, in the more than 100,000 category, we found 29% of our exporters but only 14% of non-exporters, a difference of 15 points. By comparing these percentages, we found that, in the public sector, there was a 36% lower chance of finding a personal data exporter in the category of firms with fewer than 10,000 clients, than there was of finding a respondent who reported no flows. The chance of finding the exporter in the category of firms with more than 100,000 clients was 107% greater (or double).

   This conclusion may not be surprising, given that educational institutions and hospitals often have very large numbers of clients and that public departments and organizations offering services to the general public, or to large segments of the public, may report very large numbers in response to our question. Thus, we found a shift in the size of the percentages toward higher numbers.

4. As we might expect, the situation was somewhat reversed in the private sector. Here, 46% of exporters had fewer than 10,000 clients, and 26% had more than 100,000, with only 23% falling between these two extremes. The contrasts are therefore more striking here, the "medium" categories being less populated than in the public sector. Among the "no" respondents, we found 50% of the firms with fewer than 10,000 clients and only 20% of those with large numbers of clients, i.e., more than 100,000. By comparing the percentages we find that in the private sector, a personal data exporter has only an 8% greater chance of being in the category of firms with fewer than 10,000 clients than does a respondent who reports no flows, while it has only a 30% greater chance of being in the category of firms with more than 100,000 clients. The number of clients factor therefore also affects the private sector as a whole, but to a lesser degree than the public sector.

   Graphic 2-1 shows the situation for exporters only, contrasting those that had small and medium numbers of clients with those that had large and very large numbers of clients. These variations were imperceptible when we considered the large sectors as a whole. However, they will stand out when we analyze the results in more detail by groups of sectors.

Graphic 2-1
Number of clients reported by exporters by large sector



2.2 *Results for public sector groups*

We will now analyze the size of private firms and public organizations by groups of subsectors. The tables will present the results firstly by increasing order of involvement in personal data exports (going from the least to the most) and maintaining the distinction between public and private sectors. Table 2-2 shows the following results for the public sector.

Table 2-2
Number of clients by public sector group

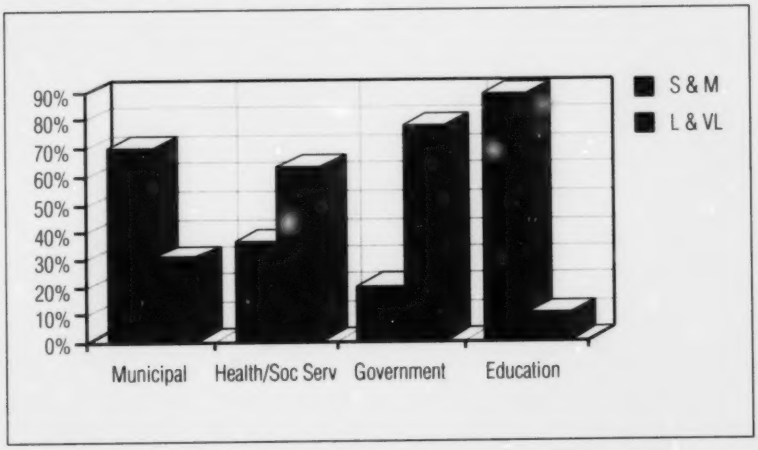
Public sector		-10,000 (%)	10-50,000 (%)	50-100,000 (%)	+100,000 (%)
MUNICIPAL	yes:	**10**	**60**	**10**	**20**
	no:	15	37	19	18
HEALTH/SOC SERVICES	yes:	**18**	**18**	**28**	**35**
	no:	56	21	7	12
GOVERNMENT	yes:	**15**	**5**	**10**	**68**
	no:	32	19	9	35
EDUCATION	yes:	**62**	**27**	**7**	**3**
	no:	69	25	3	1

1. To interpret this table, we will first examine the general situation in the public sector. Because the clients of municipalities consist of their entire population, we were not surprised to find high proportions of "yes" (70%) and "no" (56%) responses in the middle columns (from 10,000 to 100,000 people). Few municipalities with

less than 10,000 inhabitants responded and few should have been contacted. Relatively few very large municipalities responded: 20% of the "yes" (only two out of 10) respondents and 18% of the "no" (26 out of 146) respondents. The number of clients had practically no effect on whether or not there were data exports in this sector. As we already suggested, the essentially local nature of municipal activities should explain the low volumes of transborder data flows originating with respondents in this sector.

Graphic 2-2 illustrates the differences in client numbers among public sector exporters, contrasting small and medium numbers with large and very large.

Graphic 2-2
Numbers of clients of public sector exporters



2. In the health and social services field, dominated by hospitals (at least among our respondents), there is a constant progression: 18-18-28-35%. We are thus dealing with large numbers of clients in the cases of exporting institutions. Conversely, the smaller the number of clients, the less amount of data is exported, as we see from the figures in the "no" line, which this time fall from 58% for fewer than 10,000 clients, to 21%, 7% and 12% for larger numbers of clients. The number of clients variable thus had a major effect here. The contrast was particularly striking when we compared the percentages for the "yes" and "no" responses category. Exporters had a three times lower chance than non-exporters of being organizations with low numbers of clients (fewer than 10,000); however, they had practically a three times greater chance of being organizations with very large numbers of clients (more than 100,000) and an even four times greater chance of being institutions with large numbers of clients (50,000 to 100,000 persons).

3. Let us move on to government departments and organizations. Here we found the same widely varying situation involving still larger numbers of clients. A record 68% of organizations serving very large numbers of people were data exporters. The rest of the exporter category were divided among organizations with fewer clients. On the other hand, the curve for number of clients was more normal for organizations that do not export data (it reads: 32% small, 28% medium, 35% large). The number of clients is therefore of major importance in explaining the results: the proportion of exporters found in the category of public organizations with very large numbers of clients (68%) was nearly double that of non-exporters (35%), while in organizations serving small numbers of clients, the proportions were practically reversed, with only 15% exporters and 32% non-exporters in this category.
4. In the education category, we found small and medium numbers of clients: a majority of respondents were school boards and colleges, with a few universities serving larger numbers of people. The number of clients did not seem to have any effect here: 62% of the "yes" responses and 69% of the "no" responses fell into the largest category of less than 10,000 clients, not a significant difference. In the medium category (10,000 to 50,000), we found 25% and 27% respectively. In the large and very large categories, the percentages were insignificant (varying by 4% and 2%). To summarize the situation in the public sector, the number of clients was very important in health and social services and in government, but plays practically no role with respect to municipalities and education.

2.3 Results for private sector groups

Table 2-3 shows the proportions found in each private sector group.

Table 2-3
Number of clients by private sector group

Private sector		**-10,000 (%)**	**10-50,000 (%)**	**50-100,000 (%)**	**+100,000 (%)**
TRANSPORTATION	yes:	**20**	**10**	**10**	**60**
	no:	34	14	30	21
COMMUNICATIONS	yes:	**30**	**20**	**10**	**40**
	no:	58	10	6	22
FINANCE	yes:	**29**	**41**	**6**	**24**
	no:	50	25	3	19
MISC SERVICES	yes:	**60**	**20**	**0**	**10**
	no:	90	7	0	3
BUSINESS/INDUSTRY	yes:	**58**	**0**	**10**	**19**
	no:	53	13	3	24
INSURANCE	yes:	**12**	**12**	**16**	**56**
	no:	22	16	22	40
ASSOCIATIONS	yes:	**50**	**15**	**8**	**27**
	no:	42	35	17	6
COMPUTER SERVICES	yes:	**100**	**0**	**0**	**0**
	no:	95	0	5	0
PROFESSIONALS	yes:	**64**	**36**	**0**	**0**
	no:	74	17	4	0

1. In examining variations in the private sector, we will move from the subsector where we found proportionately the fewest transborder data flows to the subsector where the most were reported. First, in the transportation field where 10 respondents reported flows, six belonged to the category with the largest numbers of clients. Among respondents reporting no flows, 34% belong to the category with the smallest numbers and 30% to the next smallest numbers category. The explanatory value of the number of clients appears to be high here despite the small number of "yes" responses.

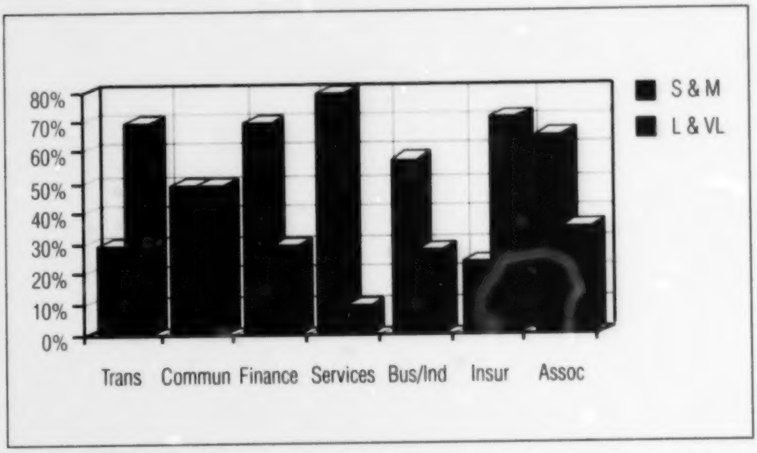
2. Communications followed nearly the same pattern. Of 10 respondents reporting flows, 40% are found in the category with the highest numbers of clients and 30% in the category with the smallest. Of those reporting no flows (67), 58% belonged to the smallest numbers category and only 22% to the largest numbers category. With the same number of respondents reporting flows (10), 60% in the miscellaneous services group had small numbers of clients compared to 10% with very large numbers (1 respondent). However, the contrast was more striking when we examined the negative responses in the miscellaneous services group: 90% were from firms with small numbers of clients compared to 3% (1 respondent) in the

over 100,000 category. Thus, in a sector where a majority of firms had small numbers of clients (allowances being made), the "no" responses occur proportionately much more often among firms with small numbers of clients than do the "yes" responses.

3. In the finance group, the numbers of clients for those who responded "yes" were better distributed among the small (29%) and extra-large (24%) categories. These proportions were, however, more varied among the "no" responses (50% as against only 19%), which was the general trend in the private sector, noted earlier. The same general pattern was found among businesses and industries, where the "no" responses go from 53% to 24%. However, there were proportionately more "yes" responses in the "small" category (58% as against only 19% in the category of firms with the largest numbers of clients).
4. Insurers are a peculiar group in that all firms had large numbers of clients; however, the numbers were still higher among personal data exporters (56%) than among non-exporters (40%). In applying this comparison to the other categories of numbers of clients, we found the reverse trend though less markedly, the 16 point lead of the "yes" responses dwindling in the medium category (to four points), in the 50-100,000 category (to six points) and in the small category (to 10 points). On the other hand, associations provide a different picture. Here a majority of exporters had small and medium numbers of clients. Exporters were proportionately more numerous among small associations (50% as against 42%) and among the large and very large (8% and 27% as against 17% and 6% non-exporters). The numbers of associations reporting no transborder data flows were proportionately higher in the medium-sized numbers of clients category (35%, as against 15% reporting flows).
5. Finally, we close this review with computer services and professionals. These groups were characterized by relatively small numbers of clients, both being concentrated in the category with less than 10,000 clients. Within the professional group, 36% were exporters and 17% non-exporters; however, these respondents fell into the "medium" category. The number of clients did not, therefore, provide an explanation in this group because our categories were relatively large (they did not discriminate below 10,000 clients) and so almost all firms fell into the first category.

Graphic 2-3 illustrates the contrasts among exporters with small and medium numbers of clients and those with large and very large numbers, by group of subsectors. Computer services and professionals are omitted because of their near absence in the large numbers of clients categories.

Graphic 2-3
Numbers of clients among private sector exporters



If we present a provisional summary for the private sector, we find that the situation is much more difficult to interpret than in the public sector because the configurations are very diverse. We shall attempt to clarify this by establishing indices that will allow us to rank our groups in increasing order, according to the influence of the number of clients on the existence of transborder data flows.

2.4 *Calculating the indices of the significance of the number of clients*

We decided to establish indices of significance for this variable, by comparing the responses in each "number of clients" category as follows. First, we considered the extreme categories: small numbers of clients (less than 10,000) and very large numbers, (more than 100,000 persons). We calculated the proportion of each category composed of exporters (the "yes" responses) in relation to the total in each category. We then compared the ratios thus obtained in each of these extreme categories, by dividing the ratio obtained in the "largest" category by the ratio in the "smallest" category. The result was an index greater or less than 1. The higher this index, the more chance there is that exporters will fall into the category with the largest numbers of clients. If it is below 1, the situation is reversed and exporters have a greater chance of falling into the category with the smallest numbers.

In some groups of subsectors, the numbers of respondents in certain categories were so low (0, 1 or 2) that there would be no purpose in calculating these ratios and indices. In these cases, we did not do the calculation and we have inserted an asterisk (*) in the table. We then weighted the results by doing a second set of calculations in which we contrasted small and medium numbers of clients against large and very large, using the same formula. Again, the result was indices above or below 1. These two indices together provide us with the range in which the number of clients has the greatest or least effect on the existence of personal data flow exports.

The following two tables provide the results of the calculation of these two sets of ratios (extreme and weighted) for each group, as well as the indices that were calculated by comparing these ratios. For both the public and private sectors, the groups are ranked by increasing size of the indices.

For the public sector, calculation of the indices yielded the following results. Column 1 of table 2-4 expresses the percentage of "yes" responses in the "small number of clients" category, column 2 the percentage of "yes" responses in the "very large number of clients" category and column 3 the index comparing these two ratios. Columns 4, 5 and 6 set out the same results for our comparison of the small and medium numbers of clients figures with the large and very large numbers figures. The results are ranked by increasing order of the weighted indices (column 6).

Table 2-4
Indices of significance of number of clients, public sector

Public sector	1	2	3	4	5	6
MUNICIPAL	*	*	*	.08	.05	0.62
EDUCATION	.22	*	*	.23	.43	1.87
GOVERNMENT	.12	.36	3.00	.11	.34	3.09
HEALTH/SOC SERVICES	.07	.41	5.86	.10	.52	5.20

As may be seen from this table, the ranking of our groups did not change whether we took the extreme indices or the weighted indices. In the municipal sector, the number of exporters was too low to provide any meaningful information. For education, the numbers were very low in the large and very large numbers of clients categories, so that the index of 1.87 must be interpreted with caution. However, in the health and social services group as well as in the government group, this factor exerts a very strong influence, with indices above 3 and 5. This means that in the government group, organizations with large or very large numbers of clients were three times as likely as organizations with small or medium-sized numbers of clients to engage in transborder personal data flows. In the health and social services group, the chances were five times higher. We may therefore deduce from this that in these two fields, the number of clients exerts a very strong influence in explaining the existence of personal data exports.

For the private sector, the calculations provide the following indices:

Table 2-5
Indices of significance of number of clients, private sector

Private sector	1	2	3	4	5	6
BUSINESS/INDUSTRY	.30	.24	0.80	.29	.22	0.76
FINANCE	.14	.25	1.78	.20	.26	1.30
ASSOCIATIONS	.39	.47	1.21	.31	.45	1.45
INSURANCE	.19	.38	2.00	.21	.33	1.57
COMMUNICATIONS	.07	.21	3.00	.10	.21	2.10
TRANSPORT/TOURISM	.05	.19	3.80	.04	.14	3.50
COMPUTER SERVICES	.37	*	*	.37	*	*
PROFESSIONALS	.35	*	*	.40	*	*
MISC SERVICES	.18	*	*	.21	*	

This table indicates that, in the computer services, professional services and miscellaneous groups, the numbers involved were too low to allow for calculation of any meaningful ratios and indices. As well, the ranking of the weighted indices followed that of the extremes because they were practically all concentrated in the small and medium numbers of clients categories.

Although the "very large number of clients" category shows proportionately fewer "yes" than "no" responses in the business and industry group and the "small" category more "yes" than "no" responses (average index below 1), this is an exception and is of little significance. Finance, associations and insurance fell around 1.5, which was quite high, indicating that, on average, one half more data exporters have very large numbers of clients than do non-exporters and one half more non-exporters have small numbers of clients. The most significant indices are found in communications and transportation: 2.1 and 3.5, respectively, and greater than 3 in the extremes category. However, we note that the ratios we worked with in these two groups were based on relatively small numbers of respondents reporting exports (10 in both cases). This comment would also apply to the miscellaneous services group referred to above.

We may therefore conclude on the basis of these indices that the number of clients is a very strong factor in explaining the existence of transborder personal data flows in the following sectors, in decreasing order of importance this time: for the public sector, in health and social services and in government; for the private sector, in transportation and tourism and in communications. This variable also has a strong influence in the areas of finance, associations and insurance. It is therefore among organizations with large numbers of clients that we find proportionately the most exporters of personal data, and conversely, non-exporters are found more often among organizations with small or medium-sized numbers of clients.

3 Number of employees

3.1 Results overall and for large sectors

We shall now consider the size of respondents' labour force or number of employees as a variable in explaining whether there are transborder personal data flows. To do this, we intend to proceed in the same manner as we did in analyzing the number of clients factor. Table 3-1 sets out the responses given by all respondents for both the public and private sectors to the question respecting numbers of employees. The "yes" responses are indicated in boldface, followed by the "no" responses in normal type, for ease in comparing and determining the explanatory value of this variable. In addition, we calculated the average for the total of 1,763 respondents. For purposes of comparison, values are indicated in percentages. Non-responses are not counted (they amounted to about 3% to 4%).

Table 3-1
Number of employees by large sector

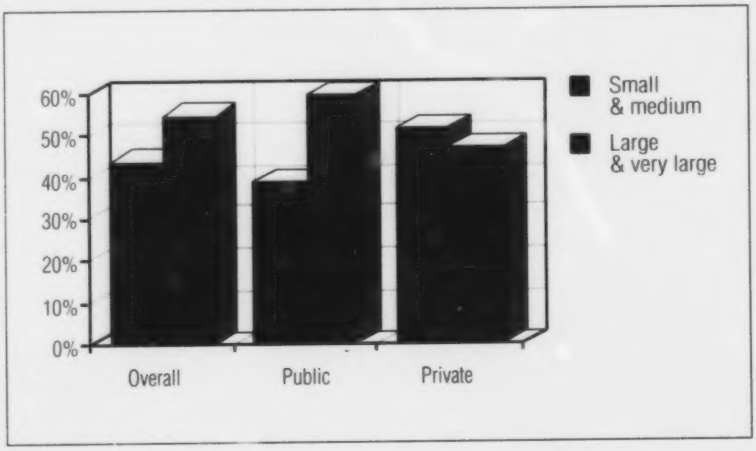
Sector		**-100 (%)**	**100-500 (%)**	**500-1,000 (%)**	**+1,000 (%)**
OVERALL	yes:	**13**	**31**	**18**	**37**
	no:	17	48	16	20
	average:	16	44	16	23
PUBLIC SECTOR:	yes:	**5**	**34**	**23**	**37**
	no:	7	55	19	19
	average:	6	51	21	23
PRIVATE SECTOR:	yes:	**24**	**28**	**11**	**36**
	no:	34	35	11	20
	average:	31	33	11	24

1. Because of the large number of "no" responses (80% overall), the average for all respondents was very similar to the average for the "no" responses, the greatest variation not exceeding 4%. We can therefore concentrate our analysis on comparing the "yes" and "no" responses.

2. If we consider all the respondents who export personal data, we found they were distributed unequally among the categories of numbers of employees. The "fewer than 100 employees" category accounted for 16% of the total on average, the "fewer than 500" accounted for 44%, the "fewer than 1,000" for only about 16% and the "more than 1,000" for 23%. This sawtooth configuration was found among all exporters ("yes"), even in the public sector where organizations of fewer than 100 employees were scarce. Transborder data flows thus occur mostly in the medium-sized (100

to 500 employees) and very large (over 1,000 employees) organizations. In total, they are distributed less unequally among small and medium-sized employers (0 to 500 employees) which together scored 44%, and the large and very large (more than 500 employees) which together scored 55%. Graphic 3-1 illustrates these findings.

Graphic 3-1
Number of employees of exporters by large sector



If we now consider the figures on the "no" side, we find that the effect of the number of employees had a considerable effect: fully 65% of these respondents employed fewer than 1,000 people while only 36% employed more than 1,000. In both cases, a difference of practically 20 points was found. We note that the difference observed in respect of numbers of clients was on the order of 12 points, indicating that the number of employees appears to be even more determinative. If we now compare these percentages, we may conclude that, in relation to a respondent who reported no flows, a personal data exporter had a 32% lower chance of being in the category of firms with fewer than 500 employees but a 53% greater chance of being in the category of organizations with more than 500 employees. We may therefore assert that the number of employees was a variable in explaining the existence of transborder personal data flows among respondents, constituting a third of our population. The more people respondents employed, the more likely they were to be exporters of personal data.

3. Let us now consider the public sector figures. For purposes of our calculations, we will deal with the first column (respondents with fewer than 100 employees) together with the second (those with 100 to 500 employees). The very low figures may be explained by the fact that we contacted municipal, educational and health services

organizations with more than 100 employees (while we did not consider this factor when we established our population of government departments and organizations). The number of people employed by some organizations must have varied downward since the data used in establishing our population was collected.

The figures we assembled and summarized in our table reflect the overall situation, but with significant variations. Only 39% of the exporters fell into the "fewer than 500 employees" category, while 62% of the non-exporters are found there. The difference of 23 points is slightly more than for the population as a whole. On the other hand, 37% of exporters fell into the "more than 500 category", while only 19% of non-exporters are found there, a difference of 18 points. This difference was almost a doubling of the percentage. By comparing the percentages, we may assert that, in the public sector, a personal data exporter was 27% less likely to be in the "fewer than 500 employees" category than a respondent reporting no flows. The respondent was more likely (or almost double) to be in the category of firms with more than 1,000 employees. This was a little lower than was found with respect to the number of clients, but it is a considerable difference.

4. The situation shows somewhat less contrast in the private sector. Here, 24% of exporters had fewer than 100 employees while 36% had more than 1,000 and 28% had a medium number of employees. The only contrast found here is in the relatively low number of firms in the "500 to 1,000 employees" category. Among the "no" respondents, we found higher percentages among small (34%) and medium-sized (35%) firms with the very large firms accounting for only 20%. Even if we add the large firms (11%) to the number of very large firms, we still have only 31% of the total "no" respondents. By comparing the percentages, we found that a personal data exporter in the private sector had a 29% lower chance of being in the category of firms with fewer than 100 employees than a respondent reporting no flows, while it had an 80% greater chance of being in the category of firms with more than 1,000 employees. The number of employees therefore had an influence on the private sector as a whole, but to a somewhat lesser extent than on the public sector.

3.2 Results for public sector groups

Table 3-2 sets out the results for number of employees for the public sector groups.

Table 3-2
Number of employees by public sector group

Public sector		-100 (%)	100-500 (%)	500-1,000 (%)	+1,000 (%)
MUNICIPAL	yes:	**0**	**60**	**30**	**10**
	no:	3	63	20	14
HEALTH/SOC SERV	yes:	**3**	**31**	**23**	**43**
	no:	6	63	17	15
GOVERNMENT	yes:	**5**	**29**	**17**	**49**
	no:	15	32	20	31
EDUCATION	yes:	**7**	**37**	**26**	**27**
	no:	4	53	21	22

We shall now examine the sizes of firms and organizations by group of subsectors. The tables of results were prepared by ranking groups by increasing order of involvement in personal data exports, going from the fewest to the most. We note that the tables do not include the percentages of non-responses.

1. Let us first examine the general situation in the public sector. Municipalities were generally not very large employers (except, of course, for large cities) so we were not surprised when we found high proportions of "yes" (60%) or "no" (63%) responses in the first two columns (fewer than 500 employees). Only one municipality with more than 1,000 employees reported engaging in transborder personal data flows. Eleven others (or 14% of the "noes") of the same size responded in the negative. However, we cannot determine a trend from so small a figure and, overall, the number of employees did not seem to influence whether there were data exports in this sector.
2. In the health and social services field, dominated by hospitals among our respondents, we found a gap between the polarization at both extremes: 43% of exporters were found in the category of more than 1,000 employees, with 34% in the "fewer than 500" category. Sixty-nine per cent of the "no" responses were found in the category of fewer than 500 employees as compared to only 15% in the "more than 1,000" category. The number of employees factor therefore had a strong influence here.
3. Let us move on to government departments and organizations. Here we found the same situation, but with less contrast. However, the numbers of employees were even larger. A record 49% of organizations that exported personal data employed very large labour forces, while only 34% of respondents reporting exports were found in the "fewer than 500 employees" category. On the other hand, the curve representing the number of employees was more normal for non-

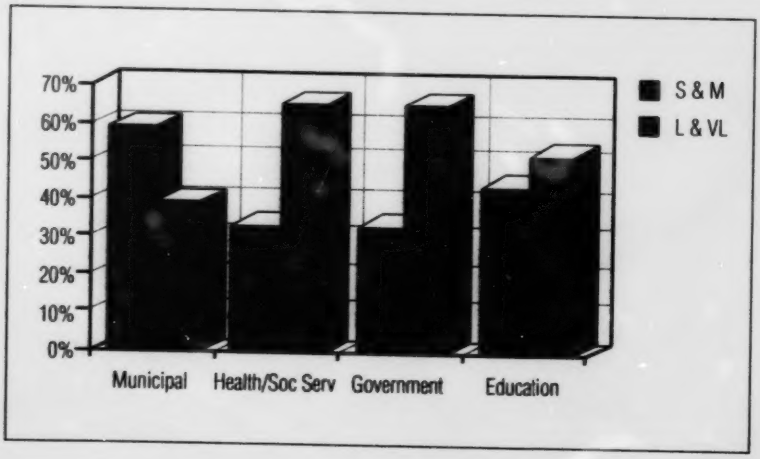
exporting organizations; it reads: 15% small (fewer than 100 employees); 32% medium-sized (between 100 and 500 employees), 20% large (between 500 and 1,000) and 31% very large (more than 1,000). The number of employees therefore seems to have moderate explanatory value. The proportion of exporters among public organizations with very large numbers of employees (49%) was more than half again as large as the proportion of non-exporters (34%). However, the proportions were practically reversed among organizations employing fewer than 500 people, with exporters accounting for 34% of this category and non-exporters for 48%.

4. In the education sector, we found the numbers of employees tend more toward the medium size, and the number of employees had relatively little influence. The proportions for the "yes" responses were 44, 26 and 27%, and for the "no" responses 57, 21 and 22%, if we combine the first two columns. For the category with the largest number of organizations, the difference of 13 points for respondents with less than 500 employees is not very significant; it is still lower in the others, with variations of only 5 points.

Our assessment of the situation in the public sector is therefore very similar to, although with fewer contrasts than, our findings for the number of clients factor. The "number of employees" variable is very important in the health and social services field, is of some importance in the government group and has practically no effect in the education and municipalities group.

Graphic 3-2 shows the differences in numbers of employees among public sector exporters, again contrasting the small and medium-sized organizations with the large and very large.

Graphic 3-2
Number of employees among public sector exporters



3.3 Results for private sector groups

1. We will now move on to examine the variations in the private sector. The results of the survey are set out in table 3-3. It will be noted first that, in the transportation group, 4 out of 10 respondents or 40% reporting flows fall into the category of the largest employers while among those reporting no flows 38% fell into the smallest employer category and 41% into the next smallest employer category. The explanatory value of the number of employees variable seems to be relatively high here, despite the small number of "yes" responses.
2. Communications closely follows the same pattern. Here again, of 10 respondents reporting flows, 40% were in the largest employers category and 40% in the smallest. Among those reporting no flows (67), only 16% were in the largest employers category. However, in the case of miscellaneous services, where the same low number of respondents reported flows (10), the opposite was true. In this category, a large majority of respondents was composed of relatively small employers (34 out of 40 had fewer than 500 employees). Thus, the trend is exactly the opposite: the "small" category accounts for 40% of the "yes" responses as against only 27% of the "no" responses. However, we should note that the "more than 500 employees" category was practically empty (six units out of 40) and that it is difficult to discern a trend.

Table 3-3
Number of employees by private sector group

Private sector		**-100 (%)**	**100-500 (%)**	**500-1,000 (%)**	**+1,000 (%)**
TRANSPORT	yes:	**20**	**40**	**0**	**40**
	no:	38	41	10	12
COMMUNICATIONS	yes:	**40**	**20**	**0**	**40**
	no:	37	45	2	16
FINANCE	yes:	**41**	**29**	**12**	**18**
	no:	48	33	3	16
MISC SERVICES	yes:	**40**	**50**	**0**	**10**
	no:	27	53	7	13
BUSINESS/INDUSTRY	yes:	**7**	**3**	**13**	**63**
	no:	5	5	25	63
INSURANCE	yes:	**20**	**36**	**16**	**28**
	no:	24	52	12	12
ASSOCIATIONS	yes:	**23**	**46**	**8**	**23**
	no:	44	42	8	4

Table 3-3
(continued)

COMPUTER SERVICES	yes:	**25**	**25**	**25**	**25**
	no:	57	24	10	1
PROFESSIONALS:	yes:	**29**	**14**	**14**	**43**
	no:	52	22	13	9

3. Looking at the finance group, we found that the numbers of employees were more equally distributed among our respondents. Among both the "yes" and the "no" responses there were relatively high numbers of small employers (41% and 48%), the medium and large numbers of employees categories together accounting for 41% and 36%, and the very large for 18% and 16%, respectively. There was practically no contrast between the "yes" and "no" responses. The same distribution was found among businesses and industries. However, this category was made up of very large employers because of the composition of our population, selected from the 500 or so largest private Canadian employers. Thus, the "very large employers" category accounts for 74% of the "yes" and 63% of the "no" responses.

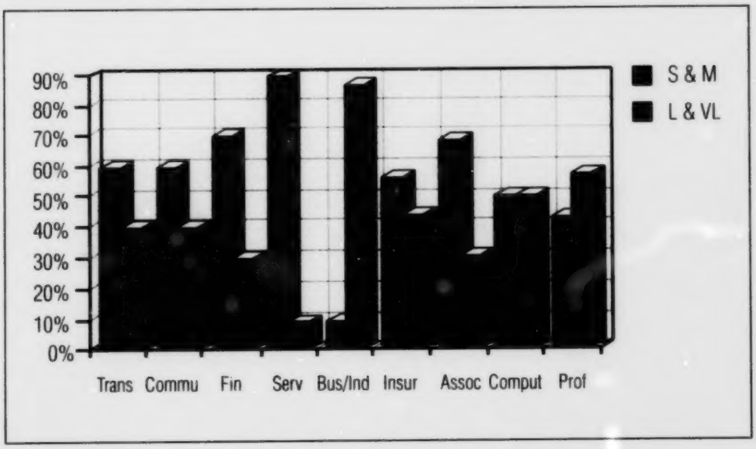
4. Insurers were relatively well distributed in all categories of employers, particularly among the "yes" responses, where the proportions were 20, 26, 16 and 28%. Among the "no" responses, we found more small employers. There was a majority of 52% in the medium-sized category of "100 to 500 employees" compared to 12% in both the "large" and "very large" employer categories. This shows a slightly greater contrast between exporters and others than did the number of clients, the proportion of firms in the "very large employer" category being more than twice as high for the "yes" responses as for the "no" responses. The situation for associations is somewhat comparable to that for the insurers: a greater majority of them were small and medium-sized employers (69% of the "yes" responses and 86% of the "no" responses). There were proportionately more exporters among large employers (23%, with six associations, as against 4% for non-exporters, only two associations in this latter case).

5. We will close this examination by looking at computer services and professionals. Contrary to the situation for numbers of clients, they showed great variation in respect of numbers of employees and were distributed throughout all four categories. For computer services, exporters were separated equally into the four categories of employers. Non-exporters were found on a sharply descending curve from the smallest (57%) to the largest (10%) firms. The distribution of exporters was different among professionals. They were relatively concentrated among very large employers (43%). Non-exporters, on the other hand, were distributed on a descending curve comparable

to the computer services curve. The number of employees factor is therefore of considerable explanatory value for these two subsectors, particularly among professionals. However, we caution that we are dealing with lower numbers of respondents than in our other subsectors (33 for computer services and 37 for professionals).

Graphic 3-3 illustrates the situation for personal data exporters in the private sector in relation to the relative numbers of employees, by group of subsectors.

Graphic 3-3
Numbers of people employed by private sector exporters



A provisional summary for the private sector would show that the situation is more difficult to interpret than in the public sector because the configurations are so diverse. In general, we found few respondents in the category of firms with 500 to 1,000 employees. We also found a concentration of small and medium-sized employers in transportation, communications, finance, miscellaneous services, associations, computer services and professionals. Only the business and industry group stands out, where a large number of respondents report having "very large numbers of employees". As a variable, "number of employees" seems to have a strong effect in groups different from those strongly affected by the "number of clients" variable. Here, associations, computer services and professionals were in the lead. We will now analyze the variations more systematically by calculating indices of significance.

3.4 *Calculation of the indices of significance of the number of employees*

We used the same method to establish tables of indices of significance for the "number of employees" variable as we used for the "number of clients" variable. The following tables set out the results of this calculation.

Table 3-4
Indices of significance of the number of employees, public sector

Public sector	1	2	3	4	5	6
MUNICIPAL	*	*	*	.06	.08	1.33
EDUCATION	*	.28	*	.20	.28	1.40
GOVERNMENT	.08	.32	4.00	.17	.28	1.65
HEALTH/ SOCIAL SERVICES	.13	.42	3.23	.11	.34	3.09

As this table shows, the ranking of our groups did not change in relation to the "number of clients" variable (table 2-4). The number of employees seems to have no effect in the municipal sector and only very little effect in the education sector. However, in the government group, this factor had a relatively large effect, although less than did the number of clients variable. (It had more effect here in the extreme categories, given the low numbers recorded in the "fewer than 100 employees" category, which creates a distortion). In health and social services, we found a high score: exporters were three times more likely to have a very large number of employees. To summarize, the "number of employees" variable had an effect mainly in the "health and social services" and the "government departments and organizations" sectors, but less effect than the "number of clients" variable.

In the private sector, the calculation of indices provides the following results:

Table 3-5
Indices of significance of the number of employees, private sector

Private sector	1	2	3	4	5	6
BUSINESS/INDUSTRY	.33	.32	0.97	.27	.28	1.04
FINANCE	.18	.23	1.28	.19	.29	1.53
INSURANCE	.26	.50	1.92	.24	.44	1.83
ASSOCIATIONS	.22	.75	3.40	.31	.57	1.84
TRANSPORTATION/ TOURISM	.04	.22	5.50	.06	.13	2.17
COMPUTER SERVICES	.20	*	*	.26	.60	2.31
PROFESSIONALS	.25	*	*	.26	.61	2.35
COMMUNICATIONS	.14	.27	1.93	.10	.25	2.50
MISC SERVICES	.33	*	*	.27	*	*

This table shows a number of shifts in the ranking of our groups, comparing the significance of the "number of employees" variable to the significance of the "number of clients" variable. The "number of employees variable" had no effect in the business and industry group, and only a moderate effect in finance (1.53). Insurers and associations were neck and neck (1.83 and 1.84) while exporters in the transportation/tourism, computer services and professional services groups were twice as likely to fall into the "large numbers of employees" category. The variable seems to have had most effect here in the field of communications, with a weighted index of 2.50. However, it should not be forgotten that the number of exporters in this group was relatively low (only 10, as in miscellaneous services, for which we could not calculate indices in view of the small numbers of respondents).

To summarize, these figures are generally comparable to our results for the "number of clients" variable. The four largest exporters (business and industry, finance, insurance, associations) remained in the same order and the "number of employees" variable had a weaker effect than in the five others where there were fewer exporters (10 for transportation and tourism, 12 for computer services, 14 for professionals and 10 for communications and miscellaneous services).

We may therefore conclude based on these indices that the "number of people employed" was a factor in whether there were exports of personal data in the following sectors (in decreasing order of importance) — for the public sector: health and social services and government; and for the private sector: primarily associations, insurance and finance and secondarily, communications, professional services, computer services and transportation and tourism.

3.5 *Summary and conclusions concerning size of respondents*

We have seen that, overall, personal data exporters are most heavily concentrated in the categories of large numbers of clients and employees, particularly in the public sector. The "number of employees" variable, however, was of less effect than the "number of clients" variable.

Looking at the groups of subsectors in the public sector, we found that these variables had the greatest effect in government, especially in health and social services. Government exporters had a three times greater chance of having large or very large numbers of clients and a 65% greater chance of having large or very large numbers of employees. In health and social services, exporters were five times more likely to have large or very large numbers of clients and three times more likely to have large or very large numbers of employees.

This phenomenon also pertains in the private sector, but it is of less importance there. The "number of clients" variable had a negative effect in business and industry and a relatively weak effect in finance (where exporters were 30% more likely than non-exporters to have large or very large numbers of clients), associations (45%) and insurers (57%) subsectors. We found practically the same order when we considered the "number of employees" variable. It had no effect in business and industry and a relatively weak effect for finance (53%), associations (84%) and insurance (83%). With respect to the other groups of subsectors, the small numbers of exporters in those groups (ranging from 10 to 14) introduced distortions into our figures. When the numbers of exporters in these categories were sufficient to calculate indices, they were in the lead, but not always in the same order. The "number of clients" variable had a very strong effect in communications and in transportation and tourism, where exporters had 2.1 and 3.5 times the chance, respectively, of being in the "large" and "very large" numbers of clients categories. Their score was equally impressive in terms of their numbers of employees, with 2.17 and 2.50 times higher chances, respectively. Computer and professional services firms also had a 2.3 times higher chance of having larger numbers of employees.

To conclude with respect to the size of the organizations, we found that the size of an organization went a long way in explaining whether there were transborder personal data flows. The "number of employees" variable, like the "number of clients" variable, also had a strong influence considering the groups of subsectors. These results seem to support our decision to direct our efforts systematically to organizations with the largest numbers of employees. It is those with the largest labour forces that most often fell into the category of personal data exporters.

4 Jurisdiction

To help ascertain respondents' basic identifying data, we asked them at the end of the first question (1e) whether their activities fell primarily under federal or provincial jurisdiction. We had a great variety of responses. Some respondents checked off both options. We will examine the results overall and then focus on the large sectors by groups of subsectors and then analyze the findings and propose interpretations.

4.1 Results overall and for large sectors

Table 4-1 sets out the results, overall and for the private and public sectors, indicating in each case the numbers of "yes" and "no" responses as well as the proportion of activities falling under federal, provincial and mixed jurisdictions.

Table 4-1
Jurisdiction by large sector

Sector		Responses	Federal (%)	Provincial (%)	Mixed (%)
OVERALL	yes:	**373**	**17**	**77**	**2**
	no:	1390	14	82	2
PUBLIC SECTOR	yes:	**211**	**5**	**92**	**0.9**
	no:	864	3	94	4
PRIVATE SECTOR	yes:	**162**	**33**	**57**	**4**
	no:	526	32	61	4

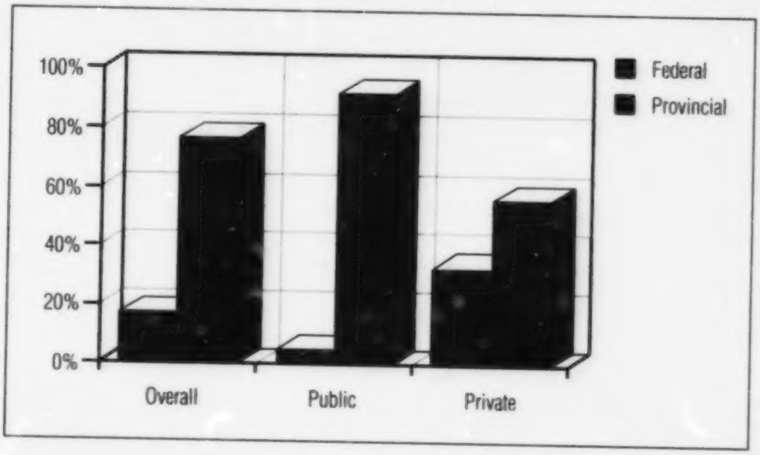
The comments that we can make on these large sectors are relatively general. We note first that, overall, a relatively modest proportion of respondents fell under federal jurisdiction: 17% of exporters and 14% of non-exporters reported that their activities were primarily under federal jurisdiction compared to 77% and 82% of exporters and non-exporters, respectively, under provincial jurisdiction. A tiny proportion of respondents (2%), concentrated in the private sector (4%), reported that their activities fell in both levels of jurisdiction. The contrasts were not as clear between exporters and non-exporters of personal data. Thus, we will go into them in more detail to discern the differences.

Comparing the public and private sectors, we can see differences even at this point. First, the distinction between the jurisdictions was clearer in the public sector, where very few respondents reported mixed jurisdictions (fewer than 1%). Next, the federal jurisdiction was strongly under-represented here, comprising only 5% of the "yes" and 3% of the "no" responses. This reflects the composition of our population, which was considerably weighted toward health and educational institutions and municipal bodies, all falling under provincial jurisdiction. We will confirm later what we have already observed with respect to the rates of response: federal departments and organizations lead in this respect. However, their participation had very little effect on the overall results.

On the other hand, when we examined the private sector results we found the situation varied more widely. Practically a third of the firms, whether or not they were exporters, surprisingly reported that they operated under federal jurisdiction. About 60% of the rest reported that their activities were under provincial jurisdiction, the balance being divided between mixed jurisdiction (4%) and no response. In order to clarify this, we first looked at what happened in our sector groups (Table 4-2). We again classified the sectors in increasing order by whether there were transborder data flows.

Graphic 4-1 shows the distribution among jurisdictions, overall and for the public and private sectors.

Graphic 4-1
Jurisdiction of exporters by large sector



4.2 *Results for public sector groups*

The results for the public sector groups are set out in the following table.

Table 4-2
Jurisdiction by public sector group

Sector		N of Responses	Federal (%)	Provincial (%)	Mixed (%)
MUNICIPAL	yes:	**10**	**0**	**100**	**0**
	no:	146	1	93	0.7
HEALTH/SOC SERV	yes:	**87**	**0**	**98**	**0**
	no:	350	1	98	0.3
GOVERNMENT	yes:	**41**	**27**	**73**	**0**
	no:	139	15	84	1.4
EDUCATION	yes:	**73**	**0**	**94**	**3**
	no:	229	2	96	0.4

The situation in the public sector is relatively simple. It confirmed that there were no exporters under federal jurisdiction in the municipal, health and social services and education subsectors. In these subsectors, some marginal respondents (on the order of 1% to 2%) reported that their activities fell under federal or divided jurisdiction.

We found the highest concentration of activities under federal jurisdiction in the government sector, 11 departments or organizations exporting data and 21 not. The proportion of exporters under federal jurisdiction was almost twice as high as for non-exporters (27% as against

15%). In this case, the fact that a respondent was a department or organization under federal jurisdiction increased the chances that it engaged in transborder data flows.

The explanation of this phenomenon probably lies in the nature of the division of powers under the Canadian Constitution, with federal departments and organizations being by nature more oriented toward matters outside Canada. However, this international orientation is not in any way exclusive. A non-negligible proportion of provincial organizations and departments also reported the export of personal data (73% or 30 units).

4.3 *Results for private sector groups*

The results for private sector groups are set out in Table 4-3.

Table 4-3
Jurisdiction by private sector group

Private sector		Response	Federal (%)	Provincial (%)	Mixed (%)
TRANSPORT	yes:	**10**	**40**	**60**	**0**
	no:	122	27	68	1
COMMUNICATIONS	yes:	**10**	**40**	**40**	**10**
	no:	67	64	34	0
FINANCE	yes:	**17**	**24**	**71**	**6**
	no:	64	27	70	2
MISC SERVICES	yes:	**10**	**30**	**70**	**0**
	no:	30	20	70	0
BUSINESS/INDUSTRY	yes:	**31**	**26**	**68**	**3**
	no:	79	24	61	11
INSURANCE	yes:	**25**	**40**	**53**	**5**
	no:	58	40	53	5
ASSOCIATIONS	yes:	**26**	**31**	**58**	**4**
	no:	48	21	63	8
COMPUTER SERVICES	yes:	**12**	**42**	**33**	**8**
	no:	12	48	48	5
PROFESSIONALS	yes:	**14**	**43**	**43**	**0**
	no:	23	13	78	4

The results are more confusing for the private sector. We found that, on average, 33% of our respondents' activities occurred under federal jurisdiction, 57% under provincial and 4% under mixed jurisdictions. The groups with more federal activity among exporters than average were: professionals (43%), computer services (42%), and insurers, communications and transportation (40% each). Those that fell below the average were: associations (31%), miscellaneous services (30%), business and industry (26%) and finance (24%). The ranking was not the same for non-exporters of personal data. Compared to a general average of 32%, the communications (64%), computer services (48%) and insurance (40%) groups were markedly higher, while transportation and finance (27% each), business and industry (24%), associations (21%), miscellaneous services (20%) and professionals (13%) were markedly below the average.

We can quickly deduce as well that the jurisdiction variable exerted greater influence where the variations between exporters and non-exporters were greatest, a higher proportion of exporting firms in the professionals, miscellaneous services, associations and transportation groups falling under federal jurisdiction, with indices of 3.31, 1.50, 1.48 and 1.48, respectively. On the other hand, the situation was the reverse for communications, where non-exporters had a greater chance of falling under federal jurisdiction, with a 1.60 index. For the other groups of subsectors, the jurisdiction variable had practically no effect: this was the case for business and industry (index 1.08 in favour of exporters), computer services (index 1.14 in favour of non-exporters) and financial services (index 1.13 in favour of non-exporters). It had absolutely no effect for insurers (index exactly 1). The distribution of mixed jurisdictions might reduce the scores for associations, computer services and miscellaneous services somewhat and even reverse the score for business and industry, but differences of only a few points were involved.

When we examine these figures in light of constitutional law, we cannot be surprised to find that federal jurisdiction was heavily present in interprovincial and international transportation, interprovincial and international communications (particularly radio and television, but also telephone and cable TV) and finance (the banks). We might also imagine that associations that are national in scope would put their activities under federal jurisdiction. On the other hand, we must seriously question the proportion of respondents who reported they operate under federal jurisdiction in the areas of computer and professional services, insurance (insurers' activities being clearly under provincial jurisdiction), business and industry, and services as diverse as advertising, personnel employment and security agencies.

By consulting the questionnaires to clarify this, we found a number of firms (and, more rarely, public organizations) which reported that their activities were mainly under federal jurisdiction. We took out those cases that appeared incongruous: a student association, insurers, a retail store, food services, a publisher, a trust company, a real estate development agency, a manufacturer of business forms, a travel agency, a mail advertising firm, a security agency, a computer dealer. How are we to explain this preference for federal jurisdiction in the reports from private sector respondents?

We must remember that the question of the division of powers between the federal and provincial governments has been the stuff of legal history for more than a century, and that the divisions are still unclear in some sectors or activities. We can then understand how, from the point of view of a firm or even a public organization that operates in one or more areas in which jurisdictions overlap or are poorly defined, it would be quite difficult to identify these activities as federal or provincial. For example, the fact that a firm was incorporated at the federal level and operated in a field under provincial jurisdiction might make it hesitate. A single firm may operate in a field in which jurisdiction is shared or in two or more fields falling under either jurisdictional level.

The incongruous responses that we have quoted undoubtedly reflect the fact that the firms in question were incorporated at the federal level (although this is not the aspect addressed by our question), or that they do business with federal agencies. Obviously, we could not go into all these explanations in drafting the questionnaire or foresee the various problems of legal classification that might arise. Thus, the responses we got to this question cannot be interpreted as totally correct, legally speaking, because of the lack of details. At most, they can provide a general idea of the jurisdictional levels under which the firms or organizations that responded operate.

4.4 *Summary and conclusions*

We have found that, overall, a relatively low proportion of respondents, about 15%, reported that their main activities took place under federal jurisdiction, while about 80% said their activities fell under provincial jurisdiction.

This proportion is tiny in the public sector (about 4%), by virtue of the composition of our population itself. However, if we isolate the government departments and public organizations, a respectable 18% of respondents fall under federal jurisdiction. The jurisdiction variable appears to be a strong explanatory factor in government departments and organizations, with exporters accounting for almost twice as high a proportion (index 1.80) as non-exporters.

On the other hand, in the private sector, a much higher proportion of respondents than anticipated, about a third of them, reported that their main activities fell under federal jurisdiction, compared to 60% under provincial jurisdiction. We must interpret these results with caution because of the difficulty in identifying certain activities as falling clearly, or mainly, under either level of jurisdiction. The groups of exporters most noteworthy with respect to federal jurisdiction were professionals, computer services and insurers (where we would have expected the opposite result) as well as communications and transportation (as we might have expected). Among non-exporters, the groups that fell most often under federal jurisdiction were again communications, computer services and insurers. The figures for others were below the average.

Finally, the "jurisdiction" variable weighed heavily on the federal side as an explanatory variable with respect to firms exporting data in the fields of professional services, miscellaneous services, associations and transportation. It was similarly weighted toward the federal side for non-exporters in the communications group.

This concludes our examination of the general characteristics of the respondents and the differences between exporters and non-exporters of personal data. The rest of our analysis will deal solely with the characteristics of the exports themselves and with the countries to which such data are exported.

PART FOUR

CHARACTERISTICS OF EXPORTS

In Part Four of our report, we examine the characteristics of the exports on the basis of the responses provided by exporters of personal data flows to countries abroad. For this purpose, we will examine, in turn: transfers to intermediaries and types of transferees; the purposes of disclosure; the volume and frequency of data flows; the nature of the data; the methods and forms of disclosure; and the protection and guarantees provided by transferees. We will conclude with a more detailed study of the 28 respondents who exported very large volumes of data. Using these cross-tabulations, based on a selection of the largest exports in terms of volume, we will then provide a general summary of the characteristics of the large-scale exports.

1 Transfers to intermediaries

In phrasing the second question of our survey questionnaire, we wanted to know whether respondents who do not themselves disclose personal data outside Canada do so through intermediaries. In that case, it would be their data that are being exported. We wanted to avoid receiving negative responses arising simply because there was an intermediary in the circuit of data disclosure. This was an effort to make the data as complete as possible and to make a full assessment of the situation.

To understand the meaning of the responses to this question, it is important that we reproduce it in full. Our analysis here will deal with the second part of this question, the first having been analyzed in point 1 dealing with the existence of transborder personal data flows.

> 2 *In the course of your operations, do you transfer data to a foreign destination, on a regular or occasional basis, concerning persons living in Canada or Canadians living abroad (by sending out such data or giving access to them)? yes ____ no ____*
>
> *If yes, please go to question 3*
>
> *If no: Do you transfer such personal data to any other Canadian firms or institutions that retransfer them beyond Canadian borders? yes ____ no ____*
>
> *If negative, please send us back the questionnaire for statistical purposes. Thanks for your cooperation!*

If yes: Is this firm or institution (please check √ your answers):

a) a telecommunications agency? ____
b) a distinct business in the information trade? ____
c) a head office or subsidiary? ____
d) a government or public institution? ____
e) other (specify) ________________________

Please answer the following questions as if you yourself were transferring these data abroad.

We found some variety in the responses to this question, which, though arranged in two parts to act as a filter, seemed to be clear and easy to answer. First, a number of respondents responded "yes" to one of the questions, but did not respond to the following questions. We indicated above that we classified these respondents in a specific category (the "yes-incompletes") and that we did not process them.

Other cases that occurred frequently: the respondent indicated "yes" in the first parts of the question but, instead of moving on to question 3 as requested, again answered "yes" to the second part of the question (transfers to other firms or organizations that retransfer abroad). To avoid duplication, we decided not to count these responses. We wanted to correctly interpret the responses given by respondents who might be in the same situation but who had followed our instructions by going on immediately to question 3, without completing the second part of the question.

In some cases, the respondents indicated in the response to the first part that they did not engage in flows, but in response to the second that they did not know whether their data were retransmitted or access given to them abroad by transferees in Canada.

In the "other" possibility at the end of question 2 (point e), three other categories, not similar to the listed four, came to our attention: transmission to the person concerned for retransmission outside the country (for example, the case of a patient who wants to obtain health care abroad and to transmit his or her medical file personally); transmission to a financial institution for retransmission; other (reference to the Canadian Bureau for International Education, CBIE). Given the marginal numbers of these responses, we simply note them here without integrating them into the calculation of our results.

Table 1-1 sets out the results from the responses to this question on intermediaries, for all respondents and for the public and private sectors. The data collected are shown as numbers of occurrences, with the corresponding percentage in parentheses.

Table 1-1
Transfers to intermediaries

Sector	Telecom (%)	Trader (%)	Head office (%)	Public Orgn (%)
OVERALL	2 (0.5)	3 (0.8)	6 (1.6)	16 (4.3)
PUBLIC SECTOR	0	1 (0.5)	1 (0.5)	14 (6.6)
PRIVATE SECTOR	2 (1.2)	2 (1.2)	5 (3.1)	2 (1.2)

There is not much information to be taken from this table because of the low numbers involved. Overall, we had 27 cases in which respondents reported they rely exclusively on intermediaries to export the firm's or organization's data, representing 7% of respondents who exported personal data. These intermediaries vary, depending on whether the exporters were in the public sector or the private sector.

Intermediaries were used most in the public sector. Out of the 16 cases identified, 14 involved transmissions to other public organizations for purposes of export. This result is not surprising, given the way in which data are organized and circulated in the public and quasi-public sectors. Some organizations must report to others (for example, the responsible government departments) on their activities and some computerized operations and processing were centralized.

We note here that some respondents reported they transmit data to public organizations but do not know whether those organizations export the data. We found only one case of transfer from the public sector to an information trading firm for purposes of exporting the data and one case of transmission to an affiliate. In the public sector subsectors, transmission via another public organization occurred mainly in educational institutions (six cases) and health and social services (seven cases). We found only one case of such transmission by a municipality. One other municipal organization transferred data using an affiliate as intermediary, and one other educational institution used a firm trading in information.

In the private sector, there was less use of intermediaries to carry out such flows and, when this was done, it was mainly through the head office or a subsidiary (five cases). There were only two cases in each of the other possibilities (telecommunications firm, trader, public organization).

We may therefore conclude from this brief examination that organizations and firms seem to be well equipped to operate in a sufficiently decentralized manner to be able to export their data themselves. However, we nonetheless identified 27 respondents who used intermediaries to export their data and who would otherwise have returned negative responses to our questionnaire. This represents 7%, not a negligible proportion in terms of assessing the situation as completely as possible.

2 Transferees

We asked the respondents to identify the types of firms or organizations to which the information they disclose abroad is transferred by checking off all the possibilities and indicating the proportion of such data that is disclosed to each type of transferee. For this purpose, we listed six types of transferees, which were designed to cover all possible data transfers. This question, number 4 of the questionnaire, read as follows:

> 4. *To which types of foreign firms or institutions do you transfer your personal data? (Please check √ all possible entries or give percentage (%) volumes if available):*
>
> *a) to a foreign part of your firm or international organization* ____
> *b) to a firm member of your group, conglomerate, etc.* ____
> *c) to a telecommunications agency* ____
> *d) to a distinct business in the information trade* ____
> *e) to a distinct private firm or individual* ____
> *f) to a distinct public institution* ____

2.1 Rate of response

The 373 respondents identified 489 possible transferees, an average of 1.31 transferee per respondent. This average was slightly higher in the public sector with 1.38 transferees, and lower in the private sector with 1.22.

However, we conclude from these data with certainty that each public sector respondent transmitted data to a larger number of transferees than was the practice in the private sector. In this respect, the interpretation we may give of these data is limited for two reasons. First, our compilation of the results does not indicate whether some persons completely declined to respond to the question. A non-response was coded but it may be interpreted in two ways: either as a negative response or as a refusal or inability to respond. These two possibilities would not have the same effect on the bases of the calculation. For purposes of our analysis, we will consider the results as if all respondents responded to this question.

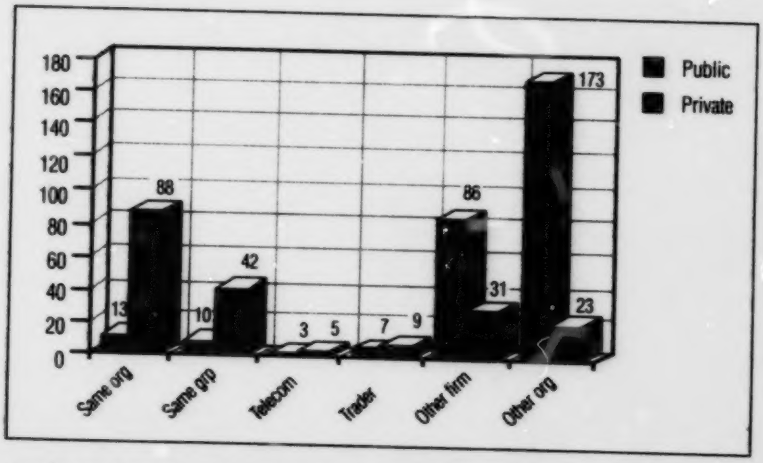
Next, because it is probable that some firms or organizations disclose data to several transferees, we asked respondents to indicate what proportion of their data disclosed abroad was transmitted to each type of transferee. We wanted to present a complete picture of the situation, showing the relative weight of the various transferees. Very few respondents gave us such figures. Out of 489 transferees reported, we identified only 39 cases in which respondents provided the percentage of data they disclose to each transferee.

Table 2-1 and Graphic 2-1 illustrate the results of the responses with respect to the types of transferees to which personal data are disclosed abroad.

Table 2-1
Types of data transferees

Type of transferee	Overall (%)	Public (%)	Private (%)
Same multinational/organization	100 (26.8)	13 (6.1)	88 (54.3)
Same group/conglomerate	52 (13.9)	10 (4.7)	42 (25.9)
Telecommunications agency	8 (2.1)	3 (1.4)	5 (3.1)
Information trader	17 (4.6)	7 (3.3)	9 (5.5)
Distinct firm or individual	196 (52.5)	173 (82.0)	23 (14.2)
No of responses/respondents	487/373	291/211	196/162

Graphic 2-1
Data transferees



2.2 *Analysis of results overall and by large sector*

The data set out in Table 2-1 show, beyond the shadow of a doubt, that the proportion of the various types of data transferees varied considerably from one sector to another. First, in the private sector, a very large majority of personal data disclosures occurred on an intra-corporate basis. In fact, more than half of the respondents stated they disclosed such data to some part of their firm (54.3%). More than a quarter of respondents (25.9%) sent such data to a firm in the same group or conglomerate. These results provide exact confirmation of the results of the earlier GRID study dealing with personal data transfers, which found that 54% of firms that transfer data abroad send them to part of their firm. Next are data transfers to a distinct firm or individual by 19.1% of respondents, followed by transfers to public organizations abroad.

In the public sector, distinct public institutions were identified by 82% of respondents as the main recipients of data transferred abroad. Next are distinct firms or individuals, which received data from 40.7% of the public organizations. A very low proportion of public sector respondents reported disclosing personal data to the four other types of transferees, fewer than 6% in each case.

One common point in both the public and private sector should be noted. Data were transferred to telecommunications agencies or firms trading in information by a very low percentage of respondents. Only 3.1% of private firms and 1.4% of public organizations report disclosing data to telecommunications agencies. Moreover, only 5.5% of the firms and 3.3% of the organizations report disclosing data to firms specializing in information trading. In the case of the public sector, these figures are somewhat reassuring, given the threat presented by the disclosure of personal data by public organizations for commercial purposes.

2.3 *Results by groups of subsectors*

1. Before analyzing the results, we note that in the private sector each respondent discloses personal data to an average 1.22 transferees. Firms in the transportation and tourism group disclose to a larger number of transferees, 2.5 per respondent on average. Professionals (1.5) and service firms (1.4) trail behind. Proportionately greater numbers of insurers (1.12), communications firms (1.10) and "others" in the finance group (0.94) transmit such data to only one transferee.

   In the public sector, where each organization discloses personal data to 1.38 transferees on average, the results vary little between the groups of organizations. The health and social services group is in the lead with an average 1.42 transferees per organization, followed by education (1.35), government (1.34) and the municipal group with 1.2 transferees per organization.

2. We now propose to analyze the results for each type of transferee. We will determine the proportion of the various groups of respondents who reported disclosing data to each type of transferee, following the order set out in our questionnaire, as reproduced in Table 2-1.

   We set out first, in order of importance, the various groups of firms that transfer data to a multinational, followed by transferees in the same group or conglomerate. In the lead are firms in the "miscellaneous services" group with 80% of respondents, followed closely by those in business and industry with 71%, transportation and tourism with 60%, computer services firms with 58%, associations with 54%, and the professional services and communications groups, with 50% each. Only in the financial field do fewer than 50% of firms transfer data to this type of transferee: 40% for the insurance group and 29% for the finance group.

Thus, we found four groups at the extremes and five groups around the average. It would be interesting to compare these results with the figures on the types of data subjects (Table 4-2). We note immediately, without going further in our analysis, that the lowest percentage of firms that transfer data about their employees and the lowest proportion that send such data to a multinational are found in the insurance and finance groups.

With respect to transfers of data to a firm in the same group or conglomerate, the results are homogeneous in five groups, with a variation from the average (29.5%) of less than 5%. The variation from the average was greater in the business and industry group, where 35% of the firms sent data to firms in the same group or conglomerate. On the other hand, only 17.6% of the finance group, 16.7% of the computer services group and 10% of the miscellaneous services group, do so.

Thus, we found the greatest proportion of firms that send data to part of their firm, or to a firm in the same group, in the business and industry sector. Next are transportation and tourism firms and service firms, where 90% of respondents transfer such data. In those cases, however, and particularly among tourism firms, this was only one of several types of transferee. The percentage of data exports sent to this type of transferee was lowest among insurers and financial firms.

We want to say a few words with respect to the 23 public organizations that reported transmitting data to "part of their firm or international organization", or to "a firm member of the same group or conglomerate". The only conclusion we can draw from the results available to us is that a majority of these organizations was in the field of education (12 out of 23). Lower numbers were in the fields of health and social services and government organizations, with six respondents each. These cases may consist of employees working abroad or individuals under exchange programs with other countries. This is the most plausible hypothesis, in our view.

3. Going on to telecommunications agencies, only eight firms or organizations transmitted personal data. With such a small number, we are obviously not surprised that there is no concentration among the sources of these disclosures. The eight firms were distributed among six groups and we can draw no conclusions from naming them. We

note only that two firms in the finance group and two organizations in education send data to such transferees.

4. The situation is somewhat different with respect to respondents who send data to firms specializing in the information trade. In the private sector, we have a category of exporters that comprised a major source of disclosures to this type of transferee: firms in the insurance group, which accounted for two thirds of these exporters (six of nine). One of these firms further reported that the data that it transferred to transferees abroad were sent to this type of transferee. These results were not surprising because health and life insurers systematically disclose data about their clients or applicants to the Medical Information Bureau. Here we mention two firms in the finance group, one tourism firm and one miscellaneous services firm, which send data to these transferees.

   Table 2-1 shows that seven public sector organizations sent data to this type of transferee: four organizations in the education field, two in the "government" group and one in "health and social services". We would need to know the reasons why these organizations are involved in such transmissions of personal data. Otherwise, any other comment would be pure speculation.

5. A total of 19.1% of firms disclose data to distinct private firms or individuals. In the lead were computer services firms (33.3%), transportation and tourism firms (30%) and firms offering professional services (28.5%). The lowest proportions of firms that transmit personal data to this type of transferee were found in the insurance group (12%) and the business and industry group.

   Moreover, a large proportion (40.7%) of public organizations reported sending data to private firms or individuals. The highest proportion of organizations that sent data to this type of transferee was found in the field of health and social services (55.9%). Four of these were also able to state the proportions of data disclosed to these transferees. Next were municipal organizations with 40%, educational organizations with 31.5%, and the government group with 24.4%. Our examination of the questionnaires permitted us to assess the volume of such data disclosures, particularly in the fields of education and health services, where numerous respondents reported transmitting such data with respect to the persons under their administration, most often at the request of individuals wishing to obtain a service, to work or to study abroad. In a majority of cases, these volumes were low, except in the health and social services field.

6. Few private firms (14.2%) sent data to a public organization abroad. Some groups of firms reported no such disclosures at all (communications and finance) while others reported very few (insurance, business and industry, miscellaneous services). On the other hand, 42.8% of professionals reported sending data to this type of trans-

feree. Next come associations (26.9%), tourism firms (10%) and computer services (16.6%).

On the other hand, public organizations abroad were the primary type of transferee for a very large majority of public sector exporters, an average of 82% of respondents overall. Organizations grouped under the "government" heading were in first place with a rate of 92.7%. Next came municipal organizations with 80%, educational organizations with 79.5%, and health and social service organizations with 77.4%. These are very high proportions. It is interesting that 12 respondents specify the proportion of all their data disclosures represented by data transmitted to this type of transferee. For seven of them, this is the only type of transferee; for three others, 80% to 99% of the data they sent to foreign transferees was sent to public organizations abroad.

2.4 *Summary and conclusions*

By identifying the types of transferees to which exporters as a whole transmit personal data, we obtain entirely different results in the various sectors. Thus, there is no purpose in analyzing the results for all respondents as a whole, other than to note that a large proportion of respondents in both sectors disclosed data to more than one type of transferee.

Public organizations sent personal data on average to a larger number of transferees than did private firms. For the public sector, organizations in the health and social services group on average transmitted data to the largest number of transferees; however, there was no significant variation from the average (1.38).

On the other hand, in the private sector we found significant differences among the various groups. Transportation and tourism dominated by far, each respondent sending data to an average 2.5 types of transferees. Respondents in the fields of finance, insurance and communications identified the smallest numbers of transferees.

With respect to data disclosures in the public sector, distinct public institutions received data from more than 80% of respondents, trailed by disclosures to distinct firms or individuals, to which more than 40% of public organizations sent data. Public institutions abroad received data from a large proportion of all organizations that responded positively to our questionnaire, but the organizations grouped under the "government" heading led the pack with a rate of more than 90%.

The largest source of data sent to distinct firms or individuals was organizations in the field of health and social services. On the other hand, only a small proportion of public organizations sent data to each of the other three types of transferees. Only a small number of organizations reported data disclosures to firms trading in information.

However, this nonetheless deserves our attention, if only to question why such transfers are made.

In the private sector, more than three quarters of respondents disclose data either to part of their multinational firm abroad (54.3%) or to a firm in the same group or conglomerate (25.9%). All types of firms are involved in this type of transfer, the finance and insurance groups showing the lowest percentage of respondents who sent data to this type of transferee. This fact is not negligible, given that these groups of firms are the initiators of large volumes of data transfers.

Distinct private firms or public institutions were identified as personal data transferees by a relatively large proportion of respondents: 19.1% and 15.9%, respectively. There was significant variation among the different groups.

These results show the importance of taking into consideration the various types of transferees in examining transborder data flows. The questions raised by these practices will certainly vary, depending on whether the data were sent in the context of intra-corporate activity or otherwise. In this respect, examination of the purpose of disclosure is a necessary complement.

3 Purposes of disclosures

We asked respondents to indicate the purposes for which they disclosed personal data to transferees abroad. In question 5 of the survey, we suggested nine possibilities and asked them to indicate all situations that applied to them. The question read as follows:

5. For which purposes is personal information being transferred abroad?
(Please check √ all possible answers):

a) Personnel management ____
b) Determination of a person's eligibility for a service ____
c) Client or membership service operations ____
d) Market research ____
e) Production of statistics ____
f) Sale & exchange of information ____
g) Application of penal or criminal provisions ____
h) Application of a law, regulation or public program ____
i) Storage of information for an undetermined later use ____
j) Other purposes (Please specify) ________________

3.1 Rate of response

Overall, respondents provided 697 responses, or an average of 1.79 responses per respondent for the public sector and 1.97 responses for the private sector, assuming all respondents completed this question. When they were asked to indicate the proportion of data transferred for each purpose reported, a very large majority of respondents failed to do so. In total, only five responses were given in percentage terms.

It is interesting that the responses to this question verified our hypothesis that any data transfer, even one that relates to a single category of people, does not necessarily have a single purpose. For example, when we asked respondents to indicate what categories of people were the subjects of the data transferred abroad, we obtained 478 responses, one quarter of respondents reporting that they transferred data about two or three categories of people. We therefore obtained one and a half times more responses with respect to purposes than we did with respect to the categories of people affected by data transfers.

3.2 *Analysis of results*

Before analyzing these results, we would like to explain briefly how we processed the responses from respondents who reported purposes of data transfers other than those listed in question 5. We made several decisions about the coding of responses that seemed to us to be similar to one of the categories listed in points a) to i) of the question. In our view, "determination of eligibility for a service" includes access to the service and insurability. We classified medical or academic follow-up with client service operations rather than with eligibility because this is a service to clients provided by the respondent, even though the foreign transferee may use the data received to determine the eligibility of the person concerned for a service.

1. The question of purpose is indisputably one of the most important issues in the protection of personal data but it is also the most complex and ambiguous. We drafted our question in as general a manner as possible, specifying various purposes, to improve the chances of getting answers. We did not wish, for example, to distinguish the purposes of the respondent firm or organization transferring the data from those of the firms or organizations receiving, processing and using the data abroad. In this regard, an educational institution that sends transcripts of marks to a foreign organization obviously does so to offer a service to its student clients who want to go abroad to study. However, for the foreign organization receiving the data, the purpose is to determine the eligibility of people for their study or scholarship programs.

   Thus the purposes overlap, depending on the point of view one takes. In processing the questionnaires, we noted that some respondents perceived this ambiguity and identified dual purposes, taking into account both their own point of view and that of the transferee. In some situations the purposes of the data exporter and transferee may coincide. For example, when a firm transfers data about its employees to its head office abroad, the known purpose in both cases is personnel management.

If we consider the number of responses received per respondent on average, we see the issue of the purposes of data transfers from a different angle, and notice that there are several possible scenarios. First, unlike the situation with respect to transferees, the greatest number of purposes of data transfers was found among private firms: on average, 1.96 purposes per firm, compared to 1.75 purposes per public sector respondent. Thus, the fact that personal data are disclosed to a single transferee does not necessarily mean that the exporter had only one purpose in doing so. The reverse is also true: a firm may disclose data to more than one transferee for the same purpose.

In this respect, it is particularly enlightening to analyze the responses obtained from each group of subsectors. We note first that respondents in five of the private sector groups had a greater number of purposes than respondents in this sector as a whole (1.96) on average. In order of importance, these were associations, in which respondents identified 2.34 purposes on average, followed by transportation and tourism firms, with an average of 2.3 purposes, computer services firms (2.16) insurers (2.07) and professionals (2.0).

Of the five groups of firms, only two were at the top of the list with respect to the number of transferees to which they send personal data: transportation and tourism firms, which transfer data to 2.5 transferees on average, and professionals, which report 1.5 transferees for their data. Respondents in the other three groups fall into the range of averages of 1.12 to 1.25 transferees for the data they report.

In the public sector, the situation is somewhat different. Although the number of transferees reported by each respondent was on average higher than for private sector respondents, the average number of purposes reported per respondent was lower than in the private sector. The only group that came close to the private sector in this respect was the government group, in which each respondent identified an average of 2.21 purposes for data transfers.

This situation may be explained in part by the fact that the composition of this group was heterogeneous, which leads to diversity in the purposes of transfers. For the other groups, organizations identified between 1.4 and 1.73 purposes each, on average. Nonetheless, this figure, which is relatively high for the public sector, may be explained in part by the fact that respondents identified dual purposes for one type of transfer, taking the transferee's point of view into account as noted earlier.

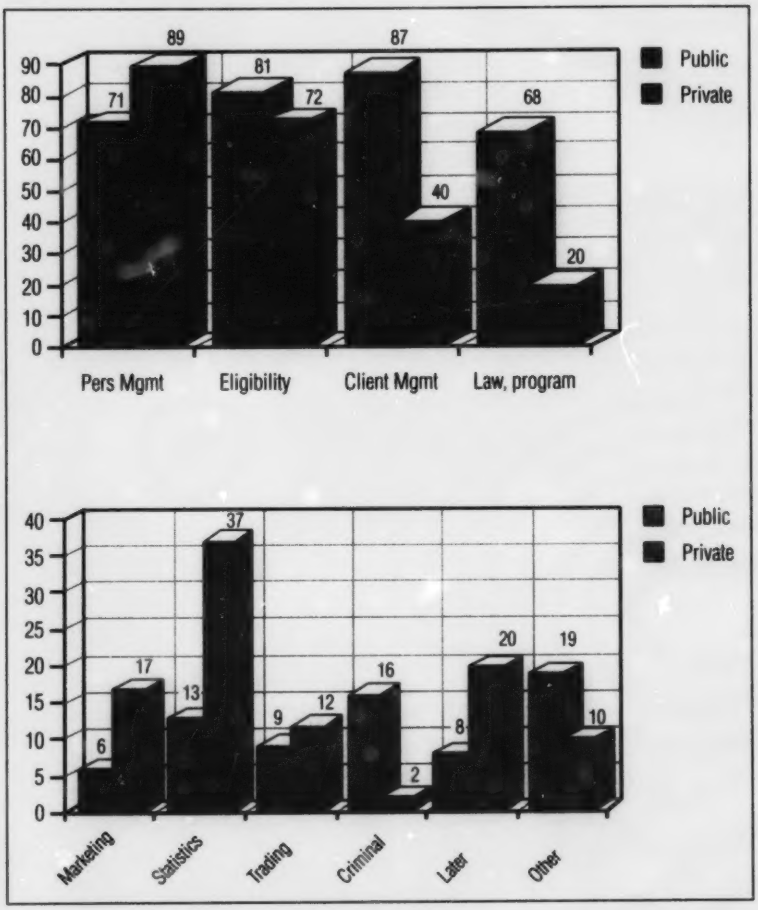
Table 3-1 and the corresponding graphic set out and illustrate the results, in numbers of responses and percentages, for the question about purposes.

Table 3-1
Purposes of disclosure

Purposes	Overall (%)	Public (%)	Private (%)
Personnel management	160 (42.9)	71 (33.6)	89 (54.9)
Eligibility for a service	153 (41.5)	81 (38.4)	72 (44.4)
Customer service operations	127 (34.1)	87 (41.2)	40 (24.7)
Marketing	23 (6.2)	6 (2.8)	17 (10.5)
Production of statistics	50 (13.4)	13 (6.2)	37 (22.8)
Trading in information	21 (5.6)	9 (4.3)	12 (7.4)
Criminal provisions	18 (4.8)	16 (7.6)	2 (1.2)
Application of law, program	88 (23.6)	68 (32.2)	20 (12.3)
Later use	28 (7.5)	8 (3.8)	20 (12.3)
Other ends	29 (7.8)	19 (9.0)	10 (6.2)
Total: responses/respondents	697/373	378/211	319/162

2. An overall view of the figures set out in Table 3-1 indicates that the three purposes that we placed at the top of the list in the question were also in the three first places for the respondents. In the private sector, they appeared in exactly the same order as in the questionnaire, while this order was reversed for the public sector. Personnel management, determination of eligibility for a service and customer service operations were therefore the three main reasons for data transfers for respondents as a whole. Next, for the private sector, came the production of statistics (22.8% of respondents) and the application of a law or program and later use (12.3% of respondents in each case). For the public sector, the only two other purposes identified by more than a tenth of respondents were the application of a law or regulation for 32.2% of the organizations, and the production of statistics.

Graphic 3-1
Purposes of exports



3. The figures for some purposes require comment or should simply be noted. More than half of the private sector respondents reported transferring data for personnel management purposes, while one third of respondents in the public sector reported doing so for the same purpose. These results are hardly surprising, because they correspond almost exactly to the figures for the number of respondents that transfer data about their employees: 63% in the private sector and 35.5% in the public sector. This means that more respondents sent data about their employees than reported data transfers for personnel management purposes.

   It can therefore be easily deduced that data transfers about employees were not all done for personnel management purposes, properly speaking, particularly in the private sector. These data were transferred for other purposes such as the production of statistics. If we consider the results obtained for each of the private sector groups, we find the same phenomenon, with the exception, however, of the insurance and tourism groups, where the same numbers of respondents reported transferring data about their employees as did so for personnel management purposes.

We found the same trend in the public sector, except for the health and social services group where we found the reverse. In that group, fewer respondents transferred data about their employees (25.3%) than did so for personnel management purposes (31%). Finally, we note that the highest proportion of firms that transfer data for personnel management purposes, 47.9% of respondents, was found in education. This is hardly surprising if we recall that 54.8% of these organizations transferred personal data about their employees.

4. In both the public and private sectors, determination of eligibility for a service was the second most common reason underlying data transfers, 38.4% and 44.4% of respondents respectively. These figures, however, cannot be taken in isolation; they must be read together with the figures for client service operations, which was the most important purpose in the public sector, with 41.2% of respondents, and the third most important in the private sector, with 24.7% of respondents.

   It is important to consider the figures for both of these two purposes together because they lead to confusion on two counts. First, although determination of eligibility for a service is a more specific purpose than client service operations, it is nonetheless a component of that purpose. However, some respondents did not necessarily perceive this distinction, which we had in fact intended to point out by listing the specific purpose before the more general. Some respondents may have preferred the general expression "client service operations" to the more specific expression "determination of eligibility for a service", even if the specific purpose was essentially why they transfer data abroad.

   And then, as we have already mentioned, these are the two purposes that may have been the main sources of confusion for respondents who were asked to report the purpose of their data transfers, their responses depending on the point of view from which they considered the purpose. A public organization that transfers data about a person under its administration, past or present, may think that it is doing something related to client service, or may think that it is transferring data to enable the transferee to determine that person's eligibility for a service. The respondent organization may even distinguish these two purposes because it sees the question from both angles at once. These considerations may certainly help to explain why a high proportion of respondents connected data transfers having these two purposes. This was so particularly in the private sector, where slightly more than half of respondents reported transferring data about their clients while, in total, more than two thirds of respondents transferred data for one or the other of these purposes.

If we consider the results for the various groups, we find that in some the same number of respondents reported transferring data about their clients as reported doing so either in order to determine a person's eligibility for a service or for client service operations. This was the case for respondents in the tourism and communications groups and in the computer services groups, respectively.

One thing is certain: it is pointless to try to find a perfect correlation between the responses with respect to the subjects of the data transfers and any one of the listed purposes, since none of them is mutually exclusive. Two examples will illustrate the various ways in which these figures can be interpreted. A respondent in the computer services group reported transferring data partly in order to determine a person's eligibility for a service and partly for client service operations, distinguishing between the specific purpose and the more general one. Others reported both purposes, even though in practice they transferred data only in order to determine people's eligibility for a service.

The accuracy of the responses given, or rather their degree of precision, depends on the respondent's perception of what distinguishes each purpose from the others. We must also avoid establishing correlations that seem to be self-evident because they are more frequent, but which are not absolute. For example, we have a tendency to connect determination of eligibility for a service with clients, but it may involve determining an employee's eligibility for a service or benefit. This seems to be the case in the "business and industry" group, where only 16.1% of respondents transferred data about their clients but 35.5% of respondents in the same group reported transferring data in order to determine eligibility for a service. Clearly, some of the data transferred relate in large part to employees' eligibility and not to that of clients.

We will briefly examine the ranking of the various groups of firms or organizations in relation to the figures for their sectors. Five groups of firms fell at about the average for the private sector (44.4%) in terms of percentage of respondents who exported personal data in order to determine eligibility for a service: insurers (60%), transportation and tourism firms (60%), computer services (58.3%), associations (53.8%) and professional services (50%).

In the client service operations category, five groups were again in the lead: computer services (50%), professional services (42.9%), associations (34.6%), communications firms (30%) and transportation and tourism firms (30%).

The figures for the public sector were relatively homogeneous in terms of the proportion of respondents who transfer data to determine eligibility for a service. Organizations in the government group were in the lead, with 53.7% of respondents. The figures for the three other groups were all close to the average for the sector as a whole (38.4%).

On the other hand, the situation is different when we examine the percentage of organizations that transfer data for client service purposes. No municipal organization reported this purpose, with only 12.2% of organizations in the government group doing so. The leading groups in this respect were therefore education (53.4%) and health and social services (49.2%).

5. Another important purpose in the private sector was the production of statistics, with 22.8% of respondents. A large percentage of respondents in the associations group (42.3%) and in each of insurance (32%) and tourism (30%) transferred data for this purpose. We might think that data transferred for this purpose were primarily being sent to part of the multinational or to a firm in the same group or conglomerate. On the other hand, the purpose cannot be connected with data transfers affecting one category of people more than another. The production of statistics may in fact be connected both with customer service operations and with personnel management or with the general management of the firm.

6. In the public sector, "application of a law, regulation or public program" is fourth in importance, with 32.2% of organizations. More than three quarters of respondents in the government group and more than a quarter of respondents in health services and the municipal group reported transfers for this purpose. In the private sector, respondents mainly in the associations sector (23.1%) and in professional services (28.6%), transferred data for this purpose. These were also the groups where we found the highest proportion of respondents who transferred data to a public organization, with 26.9% and 42.8% of respondents respectively.

7. Although only 12.3% of respondents in the private sector reported transferring data for an "undetermined later use", this percentage rose to 24% for the insurance group and about 20% for the communications and associations groups. For these respondents, this amounts to admitting that the data they transferred abroad may be used for purposes that were unknown at the time of transfer. We would note only that eight public organizations acknowledged transferring data for a purpose unknown to them.

8. Finally, we would note that a low proportion of respondents reported transferring data for the purpose of the sale and exchange of information: 7.4% of private firms and 4.3% of public organizations. This is of course a low number (nine). Nonetheless, we must question the reasons for this and attempt to identify the transferees who

received these data. We already know that seven public organizations reported transferring data to a firm that trades in information. To whom do these firms send these data in the final analysis, and to whom do the other two organizations send the data that are sent for commercial purposes? In this respect, we could not shed any light on this issue by examining all the questionnaires, because the respondents listed all types of data and transferees without connecting them to one purpose rather than another. Only qualitative interviews would enable us to go more deeply into this question.

9. To conclude, we note the nature of the "other ends" for which 29 respondents transfer data abroad. In order of importance, these were: transfers for purposes of claims or execution of judgments (12 respondents), research (four organizations), telecommunications (one) and business proposals (two), fraud prevention (one), and for purposes as specific as biographic notes for international conferences, international faculty exchanges and medico-legal purposes.

3.3 Summary and conclusions

Unlike the results we obtained with respect to transferees, private sector respondents reported, on average, the greatest number of purposes for transferring personal data abroad. Each private sector respondent reported an average of 1.96 purposes compared to the public sector figure of 1.75. This indicates that there is not always a correlation between the number of transferees to which personal data are sent and the number of purposes underlying these disclosures. The results for each group of subsectors reinforce this comment. Only two of the groups of firms that reported the largest numbers of purposes, transportation and tourism and professional services, also reported disclosing data to a high number of transferees. On the other hand, respondents in certain groups were in the lead in terms of number of purposes while, on average, they sent data to a small number of transferees. In this respect, the example of insurers is illustrative: each respondent had on average 2.34 purposes, and sent personal data to 1.12 transferees on average.

The situation is different in the public sector. The average number of transferees reported was lower (1.38) than the number of purposes for personal data transfers abroad (1.75 purposes per respondent, on average). As well, public organizations had, on average, fewer purposes (1.75) than did private firms (1.96). In this respect, organizations in the government group stand out with an average of 2.21 purposes reported per respondent. The heterogeneity of the organizations that comprise this group may help to explain this difference.

There were three reasons for a large proportion of data transfers abroad for both large sectors, although in different orders: personnel management, determination of the eligibility of the data subjects for a service, and customer service operations. In the private sector, personnel management was at the top of the list with 54.9% of respondents. This is a logical finding because 63.6% of firms transferred personal data about their employees. In the public sector, client service operations were ahead of all other purposes with 41.2% of respondents. Eligibility for a service ranks third for both sectors. Apart from that purpose, which is relatively precise in itself and which may relate both to respondents' employees and clients, the other two purposes were general and likely to overlap other more specific purposes (i.e. be a component of personnel management or client service). The same is true for the production of statistics, marketing and storage of data for later use. Some purposes, however, were more specifically associated with one sector or the other. This was the case with the application of a law, regulation or public program or the application of criminal provisions in the public sector, and with the production of statistics and marketing in the private sector.

Finally, none of the reasons listed in our questionnaire is the exclusive preserve of respondents in either of the two large sectors. For example, we found public organizations that transferred data for the purpose of trading in information, marketing or the production of statistics, just as there were firms that transferred data in order to apply a law, regulation or criminal provisions. This fact should be examined further from the point of view of protecting the rights of the subjects of these data transfers, particularly when we find public organizations reporting transfers of personal data abroad for the purposes of marketing or trading in information.

4 Volume and frequency

Clearly, our determination of the magnitude of transborder data flows must be based on the volume and frequency of such flows. In order to obtain the most precise responses possible we used different points of reference to help respondents define these factors from various angles, thus encouraging them to respond in a systematized manner.

For this reason we asked respondents to describe the status of the people who were the subjects of these disclosures: whether they were clients or persons under their administration (whom we will call "clients"), employees or other persons ("others") with whom the respondents had no relationship. By assigning these three categories at the beginning of the question relating to the volume and frequency of transfers, we hoped to help respondents identify the various possible types of transfers and thus make their assessment of volume and frequency easier, since the situation may vary from one category of people to another.

4.1 *Categories of persons who are the subjects of disclosures*

We asked respondents to indicate all categories of persons in respect of whom they disclose personal data to transferees abroad. The question was formulated as follows:

3a) Do the personal data transferred to a foreign destination pertain to your employees, your clientele, or other persons? (Please check √ all possible answers):

Clients ___ *Employees* ___ *Others* ___

4.1.1 *Multiple disclosures*

More than 99% of respondents identified categories of persons about whom data are disclosed to transferees outside Canada. In more than one quarter of these situations (26%), firms or organizations reported transferring data on more than one category of people (multiple disclosures). There was no significant difference between the public and private sectors, the percentage being higher than 25% in both cases. As well, the various scenarios occurred in the same proportion in each of the two large sectors. The most common scenario involved the disclosure of data about both clients and employees: this occurs in 70% of cases in which respondents reported disclosing data about more than one category of persons. This percentage was identical in both sectors, as the following table illustrates.

Table 4-1
Multiple disclosures scenarios

Scenario	Total (%)	Public (%)	Private (%)
Clients + Employees	67 (70.5)	38 (70.4)	29 (70.7)
Clients + Others	13 (13.7)	9 (16.7)	4 (9.8)
Employees + Others	5 (5.3)	2 (3.7)	3 (7.3)
Clients + Employees + Others	10 (10.5)	5 (9.2)	5 (12.2)
Total	95 (100)	54 (100)	41 (100)

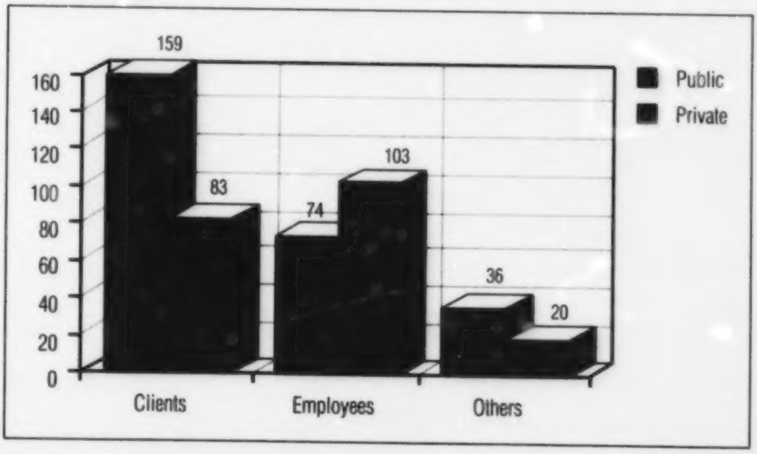
We cannot analyze the results in each of the 13 categories of firms and organizations in any greater detail because the number of respondents who reported multiple disclosures was, in most cases, too low. However, some variations should be noted. For example, more than 40% of respondents in the computer services group reported transmitting information about more than one category of people, compared to only 5.9% in the finance group and 10% in the communications and municipal groups. The situation in the other groups as a whole was much closer to the overall results, which show that 26% of firms and organizations disclosed data about more than one category of people.

In order to present a more informative and complete picture of the situation in each group, we thought it appropriate to calculate the results differently; that is, we took into account all possible configurations for transfers reported by respondents. For example, 152 respondents reported disclosing data about the clients only. On the other hand, if we add those that reported transmitting data about both clients and other categories of people, we got 242 respondents who reported disclosing data about their clients. These results are set out in Table 4-2, and illustrated in Graphic 4-1. Using them, we can highlight the major differences between the two large sectors and among certain of the large groups within those sectors.

Table 4-2
Subjects of data disclosures

Sector	Respondents	Clients (%)	Employees (%)	Others (%)
OVERALL	373	242 (64.9)	177 (47.5)	56 (15.0)
PUBLIC SECTOR	211	159 (75.4)	74 (35.1)	36 (17.1)
PRIVATE SECTOR	162	83 (51.2)	103 (63.6)	20 (12.3)

Graphic 4-1
Subjects of data disclosures



4.1.2 *Results overall and for large sectors*

On reading the data in this table, it is obvious that the situation varies enormously between the two large sectors, so that the overall results clearly do not reflect the actual situation in each sector. While 64.9% of respondents overall reported transmitting data about their clients, in fact 75.4% of public sector respondents and only 51.2% of private sector respondents did so.

The situation is reversed with respect to data disclosure about employees. In the private sector, 63.6% of respondents transmitted such data, while only 35.1% did so in the public sector. In both cases, the figures were quite different from the 47.5% average for respondents overall.

However, the difference was smaller for those respondents who disclosed data about persons other than their clients or employees: 15% overall did so, compared to 12.3% in the private sector and 17.1% in the public sector. Given these results, we need to analyze the situation by group.

4.1.3 *Results for groups of sectors*

These results for the public sector are shown in Table 4-3 and Graphic 4-2, and for the private sector in Table 4-4 and Graphic 4-3.

Table 4-3
Subjects of data disclosures, public sector

Sector	Respondents	Clients (%)	Employees (%)	Others (%)
PUBLIC SECTOR	211	159 (75.4)	74 (35.1)	36 (17.1)
Education	73	45 (61.6)	40 (54.8)	8 (11.0)
Municipal	10	6 (60.0)	2 (20.0)	4 (40.0)
Health/soc services	87	73 (83.9)	22 (25.3)	10 (11.5)
Government	41	35 (85.4)	9 (22.0)	14 (34.1)

Graphic 4-2
Subjects of data disclosures, public sector

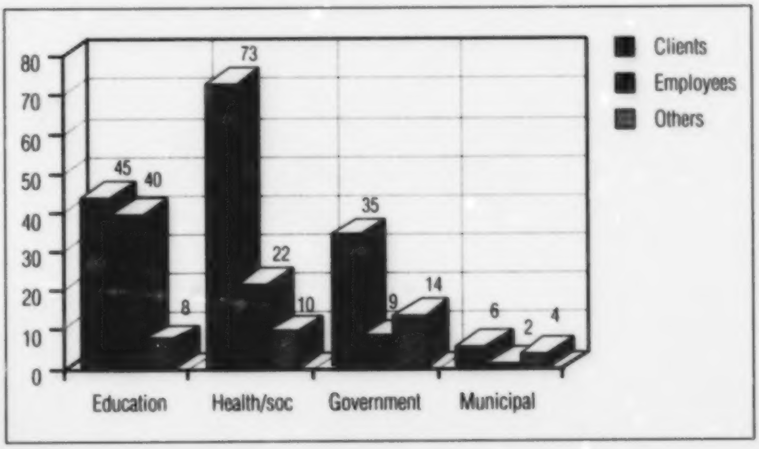
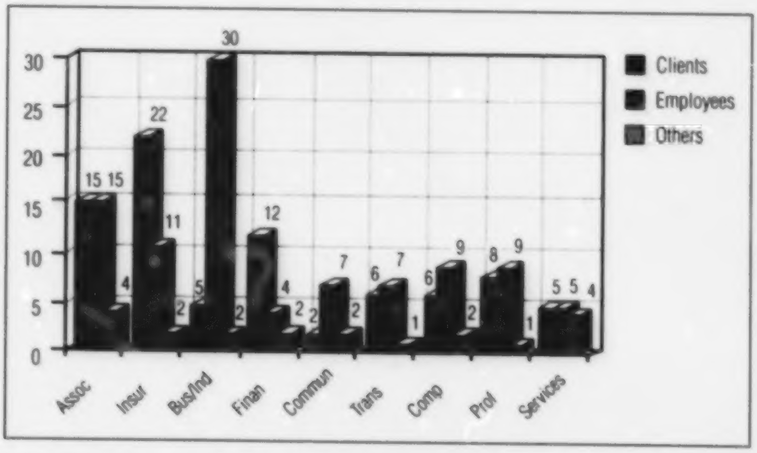


Table 4-4
Subjects of data disclosures, private sector

Sector	Respondents	Clients (%)	Employees (%)	Others (%)
PRIVATE SECTOR	162	83 (51.2)	103 (63.6)	20 (12.3)
Associations	26	15 (57.7)	15 (57.7)	4 (15.4)
Insurance	25	22 (88.0)	11 (44.0)	2 (8.0)
Business/Industry	31	5 (16.1)	30 (96.8)	2 (6.5)
Finance	17	12 (70.6)	4 (23.5)	2 (11.8)
Communications	10	2 (20.0)	7 (70.0)	2 (20.0)
Transport/Tourism	10	6 (60.0)	7 (70.0)	1 (10.0)
Computer services	12	6 (50.0)	9 (75.0)	2 (16.7)
Professionals	14	8 (57.1)	9 (64.3)	1 (7.1)
Miscellaneous services	10	5 (50.0)	5 (50.0)	4 (40.0)

Graphic 4-3
Subjects of data disclosures, private sector



1. In the public sector, it is interesting to note that the proportion of respondents who disclosed data about their clients was high in all groups, with organizations in the government and in the health and social services sectors at the top of the list, with 85.4% and 83.9% of the organizations engaging in such disclosures, respectively. On the other hand, in the field of education, almost as many organizations disclosed data about their employees (54.8%) as about their clients (61.6%). Fewer than a quarter of the organizations in the other groups disclosed data about their employees.

   We believe, however, that these results are not unexpected and that we could have obtained much higher results depending on whether or not representatives of government organizations see the citizens they serve as clients or persons under their administration. It seems realistic to us to think that some respondents identified the subjects of their data disclosures as clients, while other respondents considered them as other persons.

In the private sector, we found major differences among the groups, which we note by identifying those where the greatest variation occurred from the average for the sector as a whole. We would note first the high rate for insurers (88%) and firms operating in the field of finance (70.6%) that disclose data about their clients. On the other hand, these same sectors had the lowest percentage of firms that disclosed data about their employees. We would also note that the business and industry and communications groups had the highest proportions of respondents who reported disclosing data about their employees, 97% and 70%, respectively. These groups were also where we found the lowest percentage of respondents who transmitted data about their clients.

The results for three groups are comparable to the results for the private sector as a whole. A higher percentage of respondents in the tourism, computer services and professional services groups disclosed data about their employees, with more than half of the respondents in each group transmitting data about their clients. Finally, as many respondents in the associations and miscellaneous services groups disclosed data about their employees as they did about their clients, 57.7% and 50% respectively.

2. With respect to data disclosures about persons other than clients or employees, there are no remarkable differences in the results for the two sectors. A small proportion of respondents reported disclosing data about other persons: 17.1% in the public sector and 12.3% in the private sector. In this respect, some groups stand out because a higher proportion of the firms or organizations in those groups disclosed such data. However, in most cases, only very small numbers of respondents were involved. In the public sector, these were municipal organizations (40%) and organizations grouped under the government heading (34.1%). In the private sector, they were miscellaneous services firms with 40%, and communications firms with 20% of respondents disclosing data about "other" persons.

   In comparison with disclosures of data about clients and employees, we could conclude that this is a low percentage, but we tend rather to think that these results are much higher than we would have predicted, particularly in the public sector. This gives rise to the question of who make up this group, about whom all categories of private and public organizations disclosed data to transferees abroad. We can suggest certain hypotheses. In the communications field, they may be personalities reported in publications; in the case of associations, they may be members; for computer and miscellaneous services, it is possible that they may be employees or clients of their co-contractors; government organizations may disclose data about persons under the administration of other agencies. Finally, in all cases, they may be co-contractors. Still other hypotheses would undoubtedly cast light on this question but we cannot suggest them based solely on the results of this survey.

4.1.4 Summary and conclusions

By analyzing these results we found that a high proportion of the public sector respondents disclosed data about their clients. That sector also disclosed much lower proportional data about their employees, with the exception of organizations in the education field, which disclosed data about these two categories of people on an almost equal basis. In the private sector, the situation varies more from one group to another. Although the averages for each of the "clients" and "employees" categories of people for the sector as a whole are similar at first glance, this is because the results for certain groups counterbalance the very different results for other groups.

Thus, at one end we found the insurance and finance groups, for which the results are opposite to the results for the business and industry and communications groups. For the first, disclosures about clients were the basis of a very large majority of data disclosures to transferees abroad, while in latter groups it was disclosures about employees that predominated. However, for the five other groups, the results in each of the two large categories of subjects of data disclosures are relatively equal and, so, are much closer to the results for the private sector as a whole.

With respect to disclosures about persons other than clients or employees, it is difficult to compare the results to those for the two other categories of persons because they occurred on a much smaller scale. Despite this, the results still appear to us to be very high, particularly in the public sector where it is not easy to identify who these other persons might be, other than by suggesting certain hypotheses, as we have done.

The large variations demonstrated by our analyses of the sectors confirm that we were correct in asking people to give separate responses for disclosures about clients, employees and other persons. This enables us to target sectors by type of disclosures effected and to assess more precisely the frequency and volume of each type of disclosure.

4.2 Frequency of disclosure

4.2.1 General characteristics

After identifying the categories of persons who are the subjects of personal data disclosures, respondents were asked to indicate the usual frequency of such transfers. The question set out in 3b) of the questionnaire read as follows:

3b) Are these personal data transfers carried out on a regular or occasional basis?
regular? ___ occasional? ___ both? ___

The data set out in Table 4-5 provoke some comments, if only to point out that these responses are in themselves not very conclusive. We are not surprised to find that 75% of the representatives of public organizations indicated that such transfers took place on an occasional basis. In the fields of education and health services, which account for three quarters of the public sector respondents, data were generally transmitted at the request of the person concerned, something that was confirmed in many covering letters and explanations noted on the questionnaire.

It seems surprising, on the other hand, that only 37% of the private sector respondents transferred personal data on a regular basis, this percentage rising to 57%, however, if we consider those who reported doing so occasionally and regularly.

Our surprise is based on the fact that 60% of private sector respondents transferred data about their employees. We tend to believe that such transfers were likely to be more regular than transfers of data concerning clients. In the insurance group, where 88% of respondents transfer data about their clients and 44% about their employees, 72% report doing so on a regular basis. On the other hand, in the business and industry group, where 97% of firms disclosed data about their employees, only 22.6% of respondents reported doing so on a regular basis.

Table 4-5
Frequency of transfers

Basis	Total (%)	Public (%)	Private (%)
Regular	85 (22.8)	25 (11.5)	60 (37.0)
Occasional	225 (60.0)	159 (75.4)	66 (40.7)
Both	58 (15.0)	25 (11.8)	33 (20.4)
No response	5 (1.3)	2 (0.9)	3 (1.9)

We must therefore consider these results with great reservations. Because this is a question of perception (which depends on the respondents' concept of the regularity of transfers), it may be interpreted in a number of ways. It might, for example, be considered that transfers are regular only if the data regularly transmitted relate to the same people: for example, the same employees. Regularity might be assessed as well on the basis of the firm's normal practices. Let us take life insurance, for example. Generally, data are disclosed to the Medical Information Bureau in processing an application for insurance. This may occur only once about one person but it is an ongoing practice for the firm.

It may also be considered that transfers are "regular" if the firm or organization transfers data each time it receives a request, while other people in the same circumstances would say that these transfers occur on an occasional basis. As well, several representatives of firms that report transmitting data outside Canada only on request responded that they do not engage in such disclosures. Their questionnaires therefore fall into the "no" group. We should therefore not be surprised to encounter difficulties in interpreting the opinions of those who responded positively to this question. Fortunately, we have other data that will make it possible to determine frequency and volume of transborder data flows on the basis of uniform criteria.

4.2.2 Estimate on an annual basis

For greater precision, we asked respondents to estimate the average annual number of data transfers per person by giving a distinct response for each category of data subjects. The question set out in 3f) of the questionnaire read as follows:

3f) What is the average approximate number of data transfers per person per year?
(If less than once a year, please write -1)
(If impossible to estimate, please answer with a "?")

Clients: ____ *Employees:* ____ *Others:* ____

1. To analyze the responses, we grouped the results in one table, for respondents as a whole and for each large sector by category of data subjects: clients or persons under the organization's administration, employees and others. The figures set out in Table 4-6 include only those cases in which a precise response was provided. We thus eliminated from the analysis those respondents who did not provide any response, generally because this question did not affect them. We took the same approach for questionnaires in which the respondent was not able to specify the average annual number of transfers per person (i.e., when the respondent entered a question mark).

Thus, while 242 representatives of private firms or public organizations responded to the preceding question asking whether data about their clients or persons under their administration were disclosed, 220, or more than 90% of the respondents, answered this question. On the other hand, only 133 respondents out of the 220 affected by this aspect of the question did provide a precise estimate.

A higher proportion of respondents from private firms or public organizations that disclose data about their employees responded to this question with precise figures. While 177 respondents reported transferring such data, 169 responded to this part of the question (95.5%) and of these 124, or 73.4%, provided a precise estimate.

Finally, of the 64 respondents who transmitted data about persons other than their clients or employees, only 24 specified the average annual frequency with which they did so, giving a rate of response for analysis purposes of 37.5% (41.5% in the public sector and 30.4% in the private sector). We would also note immediately that we considered it pointless to show these figures in Table 4-6, since the results are easy to describe: in 91.6% of the cases these data were transferred less than once a year (20.8%) or once a year (70.8%). The only two cases where such data were transferred two or three times per year on average were found in the government group.

Table 4-6
Average number of transfers per year

CLIENTS (%)			**ANNUAL FREQUENCY**	**EMPLOYEES (%)**		
Overall	Public	Private		Overall	Public	Private
27 (20.3)	23 (24.5)	4 (10.2)	**less than 1/year**	22 (17.7)	18 (35.3)	4 (5.5)
72 (54.1)	47 (50.0)	25 (64.1)	**1/year**	58 (46.8)	27 (52.9)	31 (42.5)
19 (1.3)	12 (12.8)	7 (17.9)	**2/year**	12 (9.7)	3 (5.9)	9 (12.3)
4 (3.0)	4 (4.3)	——	**3/year**	6 (4.8)	1 (2.0)	5 (6.8)
2 (1.5)	2 (2.1)	——	**4-5-6/year**	5 (4.0)	1 (2.0)	4 (5.5)
1 (0.8)	——	1 (2.6)	**7-8-9/year**	——		
3 (2.2)	2 (2.1)	1 (2.6)	**10-11-12/year**	13 (10.5)	——	13 (17.8)
5 (3.8)	4 (4.3)	1 (2.6)	**more than 12/year**	8 (6.5)	1 (2.0)	7 (9.6)
133	94	39	**totals (N=100%)**	124	51	73

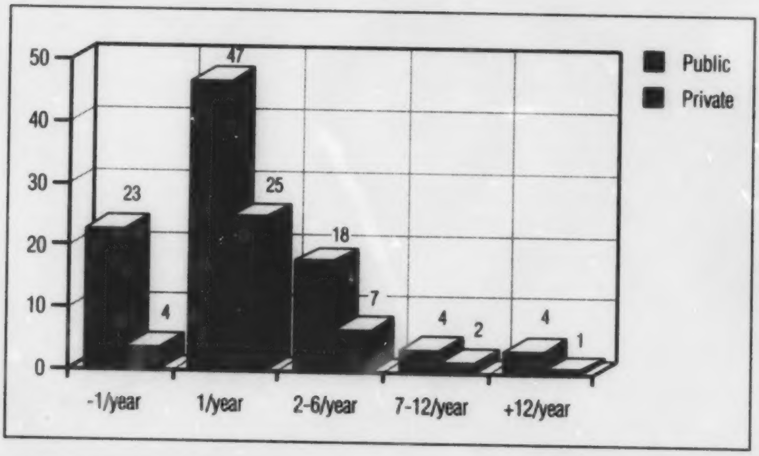
2. Transfers of data about clients occurred on average once or less per year in nearly 75% of cases for respondents as a whole. However, we found the greatest proportion of respondents who transmit such data less than once a year were in the public sector with 24.5%, compared to 10.2% in the private sector. On the other hand, 64.1% of respondents in the private sector who transfer such data do so on average once a year, compared to 50% of public sector respondents.

   We cannot analyze the private sector results specifically by subsector because there were too few responses. To do so would give us 39 responses divided into nine groups with eight levels of frequency.

   The situation is a little different for the public sector because there was a much higher number of responses, 94, which were distributed among only four groups. We note only a few items that deserve attention, indicating the limits of interpretation based on this variable alone. We have already noted the fact that 50% of the representatives of public organizations that transfer such data reported doing so on average once a year and 25% twice or more. Is this a recurring phenomenon? If so, in what situations would it be necessary for a public organization to transfer such data on so regular a basis? If we consider the data by group, we find that 65% of respondents in the health and social services group and 64% in the government group reported transferring such data on average once a year. Still more surprising are the results in the field of education, where almost half the respondents reported such transfers twice or more per year. Of course, the numbers of cases are low; nonetheless, these data are surprising.

Graphic 4-4 shows the annual frequency of data transfers concerning clients.

Graphic 4-4
Frequency of transfers concerning clients

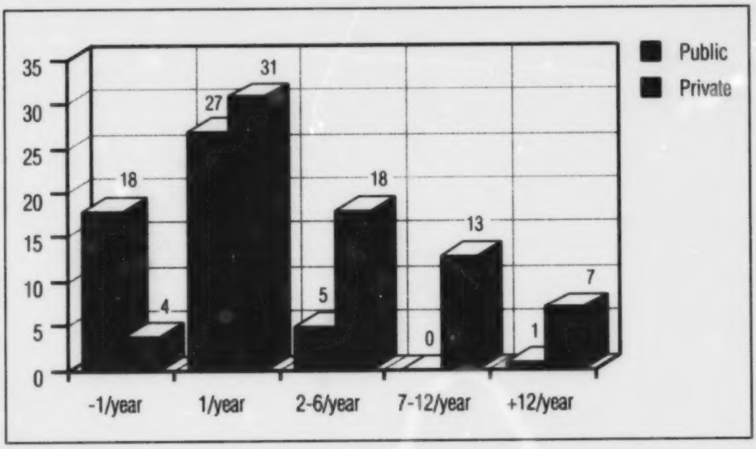


3. With respect to data transfers concerning employees, we would note that the highest proportion of respondents who report such transfers, 63%, is found in the private sector, while the percentage is 35% in the public sector. Unfortunately, only 70% of these respondents estimated the frequency of transfers.

   We would like to highlight several factors shown in the figures set out in Table 4-6. In both the public and private sectors, yearly transfers were most common: 52.9% in the public sector and 42.5% in the private. A high percentage of public organizations (35.3%) transferred such data on average less than once a year while this was the case for only 5.5% of private sector respondents. Finally, we would note that for 52% of the remaining private firms there was no clear annual average, except for firms that transfer data on their employees 10 to 12 times per year (17.8%). These were found in all groups, but more often in the business and industry and associations groups.

Graphic 4-5 shows the annual frequency of data transfers concerning employees.

Graphic 4-5
Frequency of transfers concerning employees



4. We questioned respondents with respect to the frequency of data transfers, this being one element of our mandate. The results we obtained were not in themselves very conclusive. For all categories in both sectors, the dominant frequency of data transfers was once a year. Moreover, in the public sector a relatively large proportion of data transfers respecting both clients and employees took place less than once a year. What does this mean? Apparently, it was all done on request.

   Now that we know that respondents disclose data at varying frequencies, what can we conclude? Should we, for example, be surprised that public organizations transfer data about the people under their administration more than 12 times per year? Do these transfers involve the same people? If so, we would have to know who they are and to whom and for what purposes this data is transferred. If not, this information tells us nothing because we do not know the number of people affected by the type of data disclosed.

   Are the rights that we want to protect more threatened by data transfers that occur 12 times a year, repeating or supplementing the first disclosure, rather than by one single transfer that establishes a record containing a large amount of data? We believe that the estimates of the volume of transfers will provide us with a better way of identifying the sectors of concern in terms of personal data disclosures to transferees abroad.

4.3 *Volume of transfers*

To estimate the magnitude of transborder data flows, an important variable is the volume of transfers or the number of people affected by such transfers during a specific period of time. The question concerning this variable was designed to take into account progression over time, going from a short, more recent period to a longer, more distant one. We asked the respondents to estimate the number of people affected by these data transfers, first during the last year and then during the last five years and, finally, how many people in total were affected by all of the data about them held abroad as a result of data transfers by the firm or organization.

3 c) Approximately how many individuals had their data transferred during this last year?
(If impossible to estimate, please answer with a "?")
Clients: ____ Employees: ____ Others: ____

d) Approximately how many individuals had their data transferred during the last five years?
(If impossible to estimate, please answer with a "?")
Clients: ____ Employees: ____ Others: ____

e) What would be the approximate total number of individuals whose personal data are held abroad due to transfers originating from your firm or institution?
(If impossible to estimate, please answer with a "?")
Clients: ____ Employees: ____ Others: ____

4.3.1 *Rate of response*

Our initial finding will be of no surprise to anyone. The rate of response to these questions varied greatly, depending on the length of time respondents were asked to use as the frame of reference in their estimates. The rate also varied, but to a lesser extent, according to the category of people who were the subjects of transfers and according to which of the two large sectors the respondent belonged.

To correctly assess the rate of response to these questions, we had to consider the pool of respondents affected by them (373 respondents i.e., those who transfer data about their clients [242/373], about their employees [177/373] or about other persons [60/373]), as shown by the figures in Table 4-7.

Table 4-7
Rate of response

No of subjects/time period	Total (%)	Public (%)	Private (%)
CLIENTS (N=)	242	159	83
1 year	148 (61.2)	100 (62.9)	48 (57.8)
5 years	125 (51.7)	87 (54.7)	38 (45.8)
in total	47 (19.4)	24 (15.1)	23 (27.7)
EMPLOYEES (N=)	177	74	103
1 year	135 (76.3)	53 (71.6)	82 (79.9)
5 years	113 (63.8)	53 (71.6)	82 (79.6)
in total	80 (45.2)	19 (25.7)	61 (59.2)
OTHERS (N=)	60	38	21
1 year	30 (50.0)	18 (47.4)	12 (57.1)
5 years	22 (36.7)	15 (39.5)	7 (33.3)
in total	10 (16.7)	5 (13.2)	5 (23.8)

When the questions dealt with transfers effected within the last year or last five years, a tiny minority of respondents affected by these questions (5%) completely ignored them. On the other hand, 20% ignored the question asking for an estimate of the total number of people who were the subjects of data transfers by the firm or organization. However, there were many more who were aware that the question applied to the situation in their firm or organization but were unable to estimate the number of people affected by such transfers. In order to show all these variations, we grouped the figures for the various questions in Table 4-7, by category of persons affected, for each large sector. The figures shown for "clients", "employees" and "others" represent the maximum numbers of respondents who reported disclosing data about these categories of people.

1. The figures set out in table 4-7 show that a large proportion of the representatives of firms or organizations that transferred data about their employees were able to estimate the number of people affected by such transfers. More than three quarters of them (76.3%) provided precise data on this point, the figures being 79.6% in the private sector and 71.6% in the public sector. A relatively high number of respondents, 60% of those affected, were still able to give estimates when asked to specify the number of employees affected by such transfers during the last five years. On the other hand, we found a significant drop in the rate of response when respondents were asked to estimate the cumulative number of people affected by

transfers from their firms or organizations. In this respect, we would note, however, that 59.2% of the private sector respondents were nonetheless able to provide precise figures, while only a quarter of the public sector respondents did so.

2. Again, a large proportion of respondents whose firms or organizations transfer data about clients, specified the number of persons affected by such disclosures during the last year. This time, the rate of response was highest in the public sector: 62.9% of the organizations and 57.8% of the representatives of private firms affected by this question responded.

   When the period covered by the estimate is extended to five years, it was not surprising to find that the rate of response fell somewhat; it was 8.2% less for the public sector and 12% less for the private sector. However, we found a more substantial drop in the rate of response when respondents were asked to estimate the total number of persons affected by such disclosures: 39.6% less for the public sector and 18.1% less for the private sector.

3. Scarcely half of the respondents who transferred data about people other than their clients or employees were able to estimate the number of people affected by such transfers during the last year. The response rate was 47.7% for the public sector and 57.1% for the private sector.

   We did not expect that very many organizations or firms would report disclosing data about people other than their employees or clients. In section 4.1 we found that 17.1% of public organizations and 12% of private firms, including all subsectors, reported disclosing data about such people. At that point we wondered who those people were and proposed hypotheses based on the characteristics of the various categories of respondents engaged in such transfers. We cannot say any more except to note our surprise that only a minority of these respondents was able to estimate the number of people affected by the data they transfer.

4.3.2 Transfers of data about clients

1. For purposes of analysis, we grouped the results by category of people affected by the data disclosed, to compare the results obtained on a one-year and five-year basis for each of these categories. We will examine the situation in each sector because the averages for the overall results were strongly influenced by the weight of one sector over another. For example, when we consider the figures on data transfers about clients, the public sector prevails. Because the public sector accounts for more than two thirds (67.5%) of the total responses counted, it produces a levelling off of the results, which vary greatly from one sector to the other. We will describe the volumes as follows: small volumes, (1 to 99 people); medium volumes, (100 to 999 people); large volumes, (1,000 to 9,999 people); and

very large volumes, (10,000 or more people), all on a one-year or five-year basis.

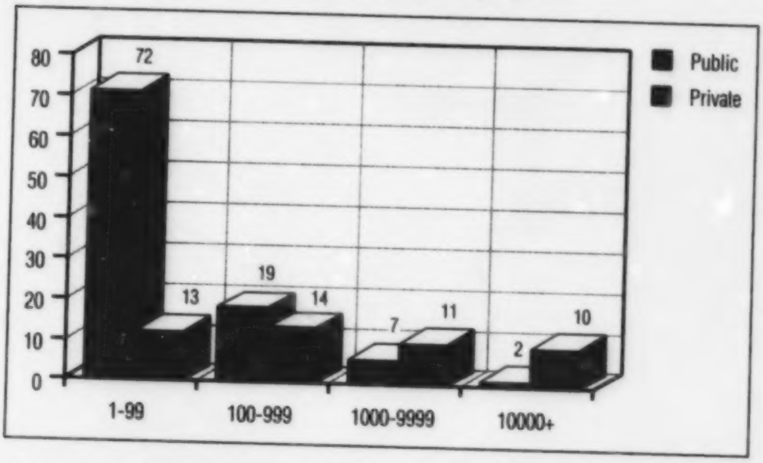
Table 4-8
Volume of transfers of data about clients

BASE: 1 YEAR (%)			VOLUME	BASE: 5 YEARS (%)		
Overall	Public	Private		Overall	Public	Private
39 (26.4)	35 (35.0)	4 (8.3)	**1 to 9**	15 (12.0)	11 (12.7)	3 (7.9)
36 (24.3)	29 (29.0)	7 (14.6)	**10 to 49**	26 (20.8)	22 (25.3)	4 (10.5)
10 (6.8)	8 (8.0)	2 (4.2)	**50 to 99**	13 (10.4)	11 (12.7)	2 (5.3)
28 (18.9)	17 (17.0)	11 (22.9)	**100 to 499**	23 (18.4)	21 (24.1)	2 (5.3)
5 (3.4)	2 (2.0)	3 (6.2)	**500 to 999**	12 (9.6)	6 (6.9)	6 (15.8)
14 (9.4)	6 (6.0)	8 (16.7)	**1000 to 4999**	14 (11.2)	9 (10.3)	5 (13.1)
4 (2.7)	1 (1.0)	3 (6.2)	**5000 to 9999**	4 (3.2)	2 (2.3)	2 (5.3)
12 (8.1)	2 (2.0)	10 (20.8)	**10000 and over**	18 (14.4)	5 (5.7)	14 (36.8)
148	100	48	**Total (N=100%)**	125	87	38

2. Let us make a summary comparison of the results for each of the sectors. One thing is clear: the volume of data transfers about clients was very low for almost three quarters (72%) of public organizations that reported transfers affecting fewer than 100 people per year. By way of comparison, barely more than a quarter (27.1%) of the private firms reported transfers dealing with so few people during the last year. These results should not be surprising, however, if we consider that the criteria used in establishing the sample operated so as to reduce the representation of small firms, something we did not do when establishing the public sector sample.

   For purposes of general comparison, we note that the private sector transfers were reported for all levels of volume. If we group the figures for the various levels, we obtain the following results: from 1 to 99, 27.1%; from 100 to 999, 29.1%; from 1,000 to 9,999, 22.9%; and 10,000 or more, 20.8%. We note that the respondents are distributed relatively equally. If we do the same thing for the public sector, we then find an entirely different situation. Only 9% of the organizations report having transferred data about 1,000 or more persons under their administration during the last year, while 19% transferred data about 100 to 999 people; it should be noted that low volumes predominated in this sector, with 72% of respondents reporting transfers of data concerning fewer than 1000 clients during the last year. Graphic 4-6 illustrates the volumes of transfers about clients for the last year.

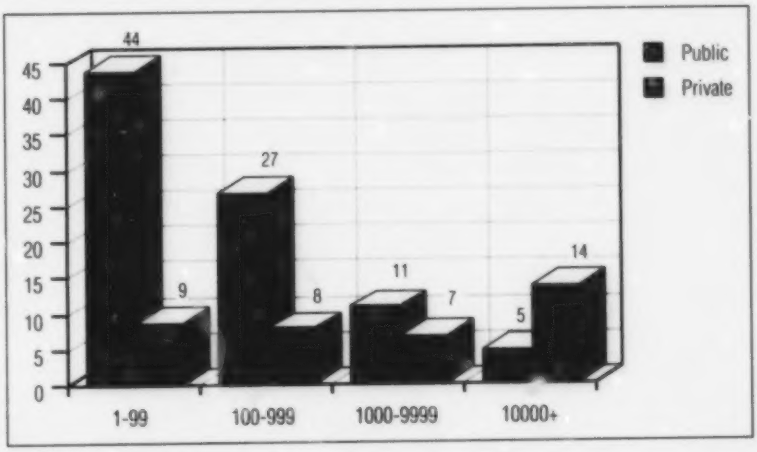
Graphic 4-6
Volumes of flows concerning clients, last year



3. The same trends appear when we consider the responses concerning transfers by respondents during the last five years. Despite the fact that the reference period is much longer, still more than half of the public organizations (50.7%) reported having transferred data about fewer than 100 clients. On the other hand, the proportion of respondents who transmitted data about more than 1,000 people almost doubled, from 9% during the last year to 18.3% for the last five years.

The results for the private sector seem at first glance to show similar consistency in terms of the distribution of respondents among the large categories, but some figures deserve attention. First, we are not surprised to find that the percentage of respondents reporting data transfers about 10,000 or more clients rose from 20.8% in the last year to 36.8% in the last five years, the number of respondents in this category having risen from 10 to 14. Still nearly a quarter of respondents (23.7%) report having transferred data about fewer than 100 clients during the last five years. The categories where there were medium and large volumes, from 100 to 999 and from 1,000 to 9,999, decreased by 8% and 4.5% respectively, with corresponding increases in the next largest categories. Graphic 4-7 illustrates these varying trends.

Graphic 4-7
Volume of flows concerning clients, last 5 years



In both the public and private sectors, we cannot establish perfect correlations between the results on a one-year basis and the results on a five-year basis because the number of respondents drops by 20% in the five-year category. Moreover, by grouping the results in eight categories we cannot verify whether there was an increase in the volume of communications during the last five years because these groups are large enough that respondents might not change category, even if the figures given on the one-year basis were multiplied by five. The only way to determine the increase in volume exactly would be to examine the questionnaires one by one to determine where the figures on a five-year basis may be the result of multiplying the figures for the last year by five. If this were the case, we could assume that there has been no increase in volume for five years.

It quickly became apparent to us that it was unrealistic to do this for 373 questionnaires. Since a more thorough examination of the questionnaires completed by respondents who transfer very large volumes of data had to be done in any event, we elected to analyze them in order to verify whether trends may be discerned in terms of increases in the volume of transfers during the last five years. Of the 25 questionnaires in which respondents reported very large volumes, only 20 could be used for this analysis: those in which respondents estimated the number of people affected on both a one-year and a five-year basis.

In half of these cases (10/20), the respondents did their five-year estimate by multiplying the number of persons affected by data transfers during the last year by five. Thus, these respondents assumed that the level of transfers had remained constant during this period. This approach was taken by seven of the 11 insurers, by two firms in the finance sector and by a medical centre.

Seven other respondents, however, submitted precise figures from which we could see that the volume of data that they transferred had increased during the last year in proportions that vary considerably from one case to another. For example, the five-year volume of transfers for two firms amounts to barely 1.5 times the volume of data transferred in the last year. In the other cases, the increase was less substantial. The respondents reporting an increase in the volume of personal data transferred outside Canada were: a government organization, two government departments, two insurers and two tourism firms. Thus, proportionately fewer respondents in the public sector (3/5) increased the volume of data transferred in the last year.

Finally, we would note three cases in which there was a decrease in the number of persons affected by data transfers during the last year: a government department, a union and a transportation firm. It is difficult to explain this for the transportation firm, which transfers data about its employees. It transferred data about seven times more people in five years than it did in the last year. Perhaps there was an unusual incidence, to say the least, of employee turnover.

The only trend revealed by these results is that the increase in volume was more evident in the public sector, while the situation appeared to be more stable in the private sector, particularly in the insurance field. However, by analyzing the results by sector we found that a significant proportion of our respondents, primarily in the public sector, disclose, and seem always to have disclosed, a low volume of personal data about their clients. In the private sector, a percentage of respondents had done so on a large scale for some time.

4. This trend, seen in the figures set out in Table 4-8, comparing the one-year and five-year figures, is confirmed by the results in terms of total volume of transfers, which appear in table 4-9. However, these figures for total volume of transfers were not defined as to time, since they were affected both by the fact that the respondents could not all speak from knowledge of practices in their firm or organization for similar periods of time and by the fact that they did not all have the same reference materials required to make such a broad estimate.

Table 4-9
Total volume of transfers concerning clients

Volume	Overall(%)	Public(%)	Private(%)
1 to 99	16 (34.0)	10 (41.7)	6 (26.1)
100 to 499	10 (21.3)	8 (33.3)	2 (8.7)
500 to 999	———	———	———
1000 to 4999	6 (12.8)	2 (8.3)	4 (17.4)
5000 to 9999	4 (8.5)	2 (8.3)	2 (8.7)
10000 to 49999	2 (4.3)	1 (4.2)	1 (4.3)
50000 to 99999	———	———	———
100000 and over	9 (19.1)	1 (4.2)	8 (34.8)
Total (N=100%)	47	24	23

Although, as we noted earlier, the number of respondents who could provide an estimate of the total number of clients affected by such transfers was low, these figures nonetheless confirm the trends already identifiable from the results covering the shorter one-year and five-year periods of time. We found the highest proportion of respondents reporting having transferred data about fewer than 500 clients in the public sector (75%), with 41.7% transferring data about fewer than 100. In the private sector, these percentages were 34.8% and 26.1% respectively.

On the other hand, the highest percentage of respondents that transferred very large volumes of data was found in the private sector: 34.8% of the 23 respondents in that sector. Only one public sector respondent reported having transferred such a large volume of data. Only an analysis of the figures for each of the 13 groups comprising the two large sectors will identify the firms or organizations involved in the various levels of volume of transfers with a reasonable degree of precision.

5. We cannot analyze the results in percentage terms for each of the 13 groups comprising the two sectors because of the low number of respondents. However, we can discern certain trends. In the private sector, we have already identified four groups where there were more respondents reporting data transfers about their clients: insurance, finance, tourism and, to a lesser extent, associations. Whether we consider the estimate given by respondents of the number of people affected by such transfers on a one-year, five-year or total basis, we still found that these were the groups in which firms

transferred data about the largest number of clients, leading us to believe that these were not very recent practices.

For example, in the insurance group, no respondent transferred data about fewer than 100 persons per year or about fewer than 500 persons in five years, and only one transferred data about fewer than 10,000 in five years. All the others (eight) in the group reported transfers about more than 10,000 clients during the last five years and five out of six transferred data about more than 100,000 clients in total. The figures in the associations and finance groups were much more scattered. Even on a five-year basis, the same number of associations transferred data about fewer than 50 people as about more than 10,000 people (two associations in each case). In the finance group, there was a little of everything, particularly when we considered the data on a one-year basis. On the other hand, for the five-year period, of four firms that provided an estimate of the number of people affected, two were responsible for transfers involving large volumes and two for very large volumes (that is, 10,000 and over).

One of the remaining groups stands out. In tourism, three firms reported transfers about more than 10,000 people on a one-year basis. On the other hand, even over a five-year period, no respondent in the five other groups reported transferring data about more than 1,000 clients. However, one retail merchant transferred data about more than 100,000 clients in total.

6. In the public sector, the heavy representation of the health and social services group had a great effect on the averages for the sector as a whole. The health and social services group accounted for 45.6% of the public sector respondents who reported transfers of data about people under their administration. The proportion for the other three groups was markedly lower: 28.7% for the education group, 21.8% for the government group and 3.8% for the municipal group. Essentially, the same proportions of respondents in the various groups provided estimates of the number of people affected by such disclosures. There is thus nothing surprising in the fact that the results for the health and social services group had a great influence on the overall public sector results, as shown by the figures set out in table 4-10.

   In this table, we have not set out the figures for the municipal group. The situation in that field is simple: the only three organizations that disclosed data about their clients did so for a small number during the last year: between 10 and 49 people. Over a five-year period, one transferred data about 10 to 49 people, one with respect to 50 to 99 people and the last with respect to 100 to 499 clients. The number of people affected was therefore small or medium.

Table 4-10
Volume of transfers about clients, public sector

BASE: 1 YEAR (%)			VOLUME	BASE: 5 YEARS (%)		
Overall	Public	Private		Overall	Public	Private
6 (22.2)	25 (49.0)	4 (20.0)	**1 to 9**	1 (4.2)	9 (20.9)	1 (5.6)
10 (37.0)	12 (23.5)	4 (20.0)	**10 to 49**	6 (25.0)	14 (32.6)	1 (5.6)
4 (14.8)	4 (7.8)	—	**50 to 99**	4 (16.6)	5 (11.6)	1 (5.6)
4 (14.8)	7 (13.7)	7 (35.0)	**100 to 499**	9 (37.5)	8 (18.6)	3 (16.6)
—	2 (1.0)	1 (5.0)	**500 to 999**	1 (4.2)	4 (9.3)	1 (5.6)
3 (11.0)	2 (3.9)	1 (5.0)	**1000 to 4999**	1 (4.2)	2 (4.6)	7 (38.9)
—	—	—	**5000 to 9999**	2 (8.3)	—	—
—	—	—	**10000 and over**	—	1 (2.3)	4 (22.2)
27	51	20	**Total (N=100%)**	24	43	18

However, we must acknowledge that the difference in the representation of the groups in this sector is relatively small because, in a majority of the cases, there were low volumes of transfers. The health and social services group had the highest proportion of respondents with transfers of personal data about fewer than 10 clients during the last year (49%). This percentage was 22.2% for the education group and 20% for the government group.

For a vast majority of public sector respondents, these transfers affected fewer than 100 persons during the last year. This was the case for 74% of the education group respondents, 80% of the health and social services group and 100% of the municipal group. Only the government group stands out, with 40% of its transfers affecting fewer than 100 persons and 40% affecting between 100 and 199 clients. This peculiarity may be explained by the fact that this group includes a range of very heterogeneous organizations, including many that centralize data on a large number of individuals.

When we consider the figures on a five-year basis, we found a predictable increase in the number of people affected by data transfers. However, it should be noted that a large proportion of respondents still reported transfers of data about fewer than 100 persons (65.1% in the health and social services group and 45.8% in the education group) and that more than 85% of the organizations in these groups transferred data about fewer than 1,000 clients. These figures show a certain consistency over the last five years.

Finally, we would note that five organizations, four of which were in the government group, transferred data about more than 10,000 persons during the last five years and that two in the education group did so for more than 5,000 clients. Given the size of these volumes, these situations should clearly attract our attention when we consider the countries of destination, to determine whether such transfers are being made to specific countries more than others.

Clearly, a large majority of public organizations transfer data about a small number of clients. On a one-year basis, 72% of the organizations transferred data about fewer than 100 people and, if we include transfers involving fewer than 1,000 people, the figure is 91%. Even on a five-year basis, the proportions of small and medium volumes remain high, with 50.7% and 81.7% of organizations, respectively, transmitting such small volumes of data.

In the private sector, the situation is somewhat different. Respondents were distributed relatively equally among the four volume levels. During the last year, firms that transferred small and medium volumes led, with 27.1% and 29.1% of respondents, respectively; nonetheless, 22.9% and 20.8% of firms transferred data about a large or very large number of clients during that year. On a five-year basis, the picture is a little different. The proportion of respondents transferring data about a small number of clients remained stable, but the proportion of respondents who transferred very large volumes increased substantially from 20.8% to 36.8%.

It is primarily in the groups of subsectors with the most firms that transfer data about their clients that we found the greatest number of respondents who transfer large and very large volumes of data. They are found first and foremost in the field of insurance, followed by the transportation and tourism subsectors and, finally, in a much smaller proportion, in the finance subsector, for which it will be recalled we had a very low response rate among the financial institutions that are, in our opinion, most likely to transfer data abroad.

4.3.3 *Transfers of data about employees*

1. We have already noted that 63.6% of private sector respondents and 35.1% of public sector respondents reported transferring data about their employees. Of these, 79.6% and 71.6% respectively provided an estimate of the number of people affected by such transfers during the last year and nearly 65% did so on a five-year basis. We grouped these figures in table 4-11, showing the situation in each sector, followed immediately by Table 4-12 setting out the figures for the total numbers of employees affected by transborder data transfers.

Table 4-11
Volume of transfers dealing with employees

BASE: 1 YEAR (%)			VOLUME	BASE: 5 YEARS (%)		
Overall	Public	Private		Overall	Public	Private
53 (39.3)	35 (66.0)	18 (22.0)	**1 to 9**	31 (27.4)	27 (56.3)	4 (6.2)
39 (38.9)	11 (20.8)	28 (34.1)	**10 to 49**	29 (25.7)	10 (20.8)	19 (29.2)
15 (11.1)	2 (3.8)	13 (15.9)	**50 to 99**	16 (14.2)	5 (10.4)	11 (16.9)
21 (15.6)	5 (9.4)	16 (19.5)	**100 to 499**	25 (22.1)	5 (10.4)	20 (30.8)
1 (0.7)	——	1 (1.2)	**500 to 999**	7 (6.2)	1 (2.1)	6 (9.2)
6 (4.4)	——	6 (7.3)	**1000 to 4999**	3 (2.6)	——	3 (4.6)
——	——	——	**5000 to 9999**	1 (0.9)	——	1 (1.5)
——	——	——	**10000 and over**	1 (0.9)	——	1 (1.5)
135	53	82	**Total (N=100%)**	113	48	65

Table 4-12
Total volume of transfers dealing with employees

Volume	**Overall (%)**	**Public (%)**	**Private (%)**
1 to 99	49 (61.3)	15 (78.9)	34 (55.7)
100 to 499	20 (25.0)	1 (5.3)	19 (31.3)
500 to 999	1 (1.2)	——	1 (1.6)
1000 to 4999	7 (8.8)	3 (15.8)	4 (6.6)
5000 to 9999	——	——	——
10000 to 49999	3 (3.7)	——	3 (4.9)
Total (N=100%)	80	19	61

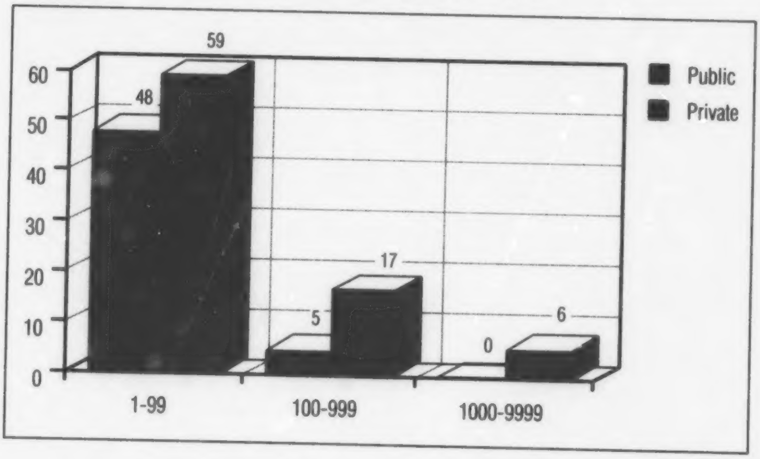
2. On examining these figures, we see first that two thirds of the public sector respondents transferred data about fewer than 10 employees during the last year, and that more than 90% of respondents transferred data about fewer than 100 employees during the same period. Those respondents who transferred data about more than 100 employees are found in the fields of education (4) and health services (1). These are also the fields in which there was the greatest likelihood of international exchanges for training and cooperative purposes.

   If we consider the volume of transfers during the last five years, the number of people affected remains below 100 for 87.5% of respondents. Again, we find slightly larger volumes in the field of education, three respondents transferring data about more than 100 employees and one about more than 500. Two organizations or departments broke the 100 ceiling over a five-year period.

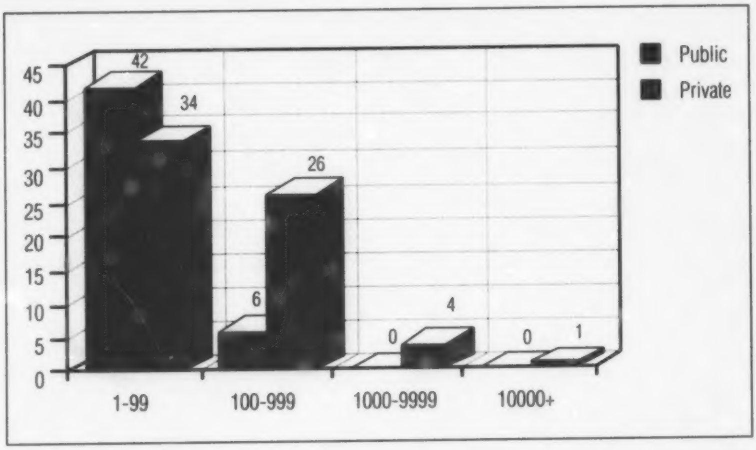
Finally, we would note that only 18 representatives of public organizations provided an estimate of the total number of employees affected by the data disclosed to transferees abroad. As the figures in table 4-12 show, in almost 85% of the cases the volumes remained small and medium. Only one organization in the education field and two in the government group transferred data about more than 1,000 employees in total.

Graphic 4-8 illustrates the volumes of transfers dealing with employees on the basis of the last year; graphic 4-9 does so on a five-year basis.

Graphic 4-8
Volume of flows concerning employees, last year



Graphic 4-9
Volume of flows concerning employees, last five years



3. The situation in the private sector differs somewhat from what we observed in the public sector. This should not be surprising, considering that the reasons for the data transfers dealing with employees were different most of the time from the reasons in the public sector. We will return later to these reasons, after we have ascertained the types of transferees to which firms sent these data or the purposes for which they did so.

The fact that there are some variations among the figures for each of the sectors is hardly surprising; on the other hand, we might be surprised that they are not larger (see table 4-11). In fact a very large percentage of respondents (72%) reported having transferred data about fewer than 100 employees during the last year, while only 24% of respondents in the private sector had fewer than 100 people in their employ. In addition, 7.3% of respondents transferred data about 1,000 employees or more.

On a five-year basis, the number of persons affected by these transfers was obviously higher. There were 20% fewer respondents who transferred data about fewer than 100 employees during the last five y[illegible]52%) and 20% more who transferred data about 100 to 999 [illegible]ple (40%). However, there were still four firms that transferred data about fewer than 10 employees. The percentage of respondents who transferred data about more than 1,000 employees remained at a little more than 7%, with only one firm having broken the ceiling of 10,000 over five years.

We now consider the distribution of the various groups of firms that transfer data about their employees. First, on a one-year basis, all types of firms except those in the finance sector were involved in transfers affecting fewer than 100 employees. This is hardly surprising because the total percentage of firms concerned was very high. For transfers involving 100 to 499 employees, the business and industry fields predominate (5), followed by insurance, finance and professionals (three each) and by communications and computer services (one each). One association reported transfers about 500 to 999 employees. Among the largest, we found one firm in the insurance field, one in business and industry, one in tourism and two computer services firms.

The figures on a five-year basis change the outcome very little. There seems to have been a simple rollover of respondents into the next category, given that the estimate now relates to a longer period. We can only deduce from this that respondents multiplied the earlier figure on a one-year basis by five. This appears logical because, unless there was an incredible turnover of personnel, it would largely be the same employees who were affected by these transfers during the five-year period. We would note, however, that there appear to be exceptions. One representative in the computer services field went from more that 1,000 to more than 5,000 people, and another in tourism went from more than 1,000 to more than 10,000. Two representatives in insurance and one in business and industry each remained in the 1,000 to 4,999 category of people affected over five years.

We will close with a brief overview of the estimates given by respondents of the total number of employees affected by data disclosed to transferees abroad. The figures show that the results differ little from what we found for the five-year estimate. Again we have 34 private sector respondents who reported total data transfers concerning fewer than 100 employees. The only category that seems to have changed is the more than 10,000, where we found three respondents (compared to one in this category for the five-year period), one in insurance and two in business and industry. No respondent reported transferring data about more than 50,000 employees.

In conclusion, three private sector groups dominate in terms of the number of firms that transfer data about their employees: business and industry, associations and insurance. However, a majority of the firms in these groups transferred small and medium volumes of data. These firms, as well as those in the tourism and computer services fields, had the most respondents who transferred data about more than 1,000 employees per year. Finally, we note that in the finance group, neither very large nor small volumes were reported, while only very small volumes were reported in the services group. These were the two fields in which we found the fewest respondents who transfer data about their employees.

4.3.4 *Transfers of data about "other" persons*

1. As we have seen, only a tiny minority of respondents transferred data about people other than clients, persons under the administration of an organization, or employees. Paradoxically, we found the highest proportion of respondents who reported this kind of transfer in the public sector, with a rate of 18% compared to only 11.7% in the private sector. In table 4-13 we grouped the responses of the organizations or firms that estimated the number of people affected by such transfers on a one-year and five-year basis.

Table 4-13
Volume of transfers dealing with other persons

BASE: 1 YEAR (%)			VOLUME	BASE: 5 YEARS (%)		
Overall	Public	Private		Overall	Public	Private
10 (33.3)	6 (33.3)	4 (33.3)	**1 to 9**	5 (22.7)	3 (20.0)	2 (28.6)
10 (33.3)	8 (44.4)	2 (16.7)	**10 to 49**	7 (31.8)	5 (33.3)	2 (28.6)
1 (3.3)	——	1 (8.3)	**50 to 99**	2 (9.1)	2 (13.3)	——
3 (10.0)	2 (11.1)	1 (8.3)	**100 to 499**	3 (13.6)	2 (13.3)	1 (14.3)
——	——	——	**500 to 999**	1 (4.5)	——	1 (14.3)
3 (10.0)	1 (5.6)	2 (16.7)	**1000 to 4999**	1 (4.5)	1 (6.7)	——
2 (6.7)	1 (5.6)	1 (8.3)	**5000 to 9999**	1 (4.5)	1 (6.7)	——
1 (3.3)	——	1 (8.3)	**10000 and over**	2 (9.1)	1 (6.7)	1 (14.3)
30	18	12	**Total (N=100%)**	22	15	7

2. In the public sector, a total of 38 organizations that reported transferring such data were distributed as follows among the four groups: government, 14; health and social services, 12; education, nine; and municipal, three. Only 18 of these stated the number of people affected by such transfers during the last year and 15 during the last five years. In more than three quarters of the cases (77.7%), a small number of people, fewer than 50, were affected by these transfers. Two organizations, one in health and social services and one in education, transferred data about 100 to 499 people during the last year. Finally, two organizations in the government group transferred data about more than 1,000 people in the same period.

   Over a five-year period, the situation seems to have changed little; 80% of public sector respondents reported having transferred such data about fewer than 1,000 people. The highest volumes were found in the same groups.

3. In the private sector, 19 respondents reported that their firms disclosed data about "other" people to transferees abroad. These respondents were distributed among the nine groups; however,

some were more heavily represented: commerce and industry, with five firms; associations and miscellaneous services, with three respondents each; two in the insurance group; two in communications; and one in each of the other four groups — finance, tourism, computer services and professionals.

Only 12 of these respondents specified the number of people affected by such transfers and, as the figures set out in Table 4-13 illustrate, these volumes were very small in 50% of the cases. Only four respondents reported transferring large volumes of data. One insurer and one association transferred data about more than 1,000 people this year, another insurer did so with respect to more than 5,000 people, and one services firm involved in direct marketing with respect to more than 10,000.

4.4 *Summary and conclusions*

On analyzing the figures for the questions on volume and frequency, we are led to an initial observation. We were correct in asking the participating firms and organizations to identify the categories of persons about whom they transfer personal data abroad and to estimate the frequency and volume separately for each category of data subjects. Not only are the results very different for each of the sectors, but we also find significant differences among the groups that make up these sectors and in the different categories of people affected by the data transfers.

In the public sector, a very large majority of respondents, more than three quarters, transferred data about people under their administration, and a smaller proportion of organizations also transferred data about their employees. Except for organizations in the education field, almost the same number transferred data about each category of persons. Private sector firms transferred data about their employees more often than they did about their clients. However, when we consider the figures for each of the nine groups in this sector, we found that this average reflects the situation among only one segment. Business and industry show the highest proportion of firms that transfer data about their employees and a much lower proportion that do so about their clients. Of the other groups, data transfers about clients were most common: this was the case for firms in the insurance and finance groups. In the other private sector groups as a whole, there was much less variation between the percentage of firms transferring data about these two categories of persons.

Overall, the proportion of firms or organizations that transfer data about "other" persons was relatively low. Paradoxically, we found the highest proportion of respondents who transfer such data in the municipal and "government" groups. These results cannot be explained using only the results of our study because there is nothing to indicate who these third persons might be.

By using the categories of persons affected to analyze data transfers, we get a more accurate and detailed picture of the situation in each of the large sectors. While this is of less benefit when we consider the frequency of transfers, it is nonetheless clearly useful when we analyze the volume of data transfers. Respondents who transferred data about their employees were more able to estimate the frequency of such transfers and numbers of people affected by them than were those who transfer data about their clients. In the public sector, the situation was reversed. Overall, proportionately more respondents in the public sector gave such estimates than did private sector respondents.

Few differences are evident with respect to frequency of transfers, except that in the private sector a significant proportion of data transfers concerning employees (48%) occurred more than once a year, while only 25% of transfers concerning clients of firms occurred as frequently. In the public sector, fewer than a quarter of transfers occurred more frequently than once a year, whether with respect to employees or clients. This variable offers little assistance in understanding the magnitude of transborder data flows. In this respect, the volume of transfers clearly had a more determinative effect.

If we consider the volume of transfers, the impact of some of our other figures is reduced or, at least, they are put in proper perspective. We already noted that the proportion of private firms that disclosed data about their clients was lower than the proportion that disclosed data about their employees. In the private sector, data transfers about clients generated the largest volumes of transfers. The subsectors where we found the highest proportion of firms that transfer data about their clients produced the largest volumes of data transfers. Firms in the insurance group dominated, with seven insurers that transferred data about 10,000 to 200,000 clients during the last year and more than 10 that did so with respect to more than 10,000 in the last five years. Next was transportation and tourism group, where three firms transferred data about more than 50,000 clients during the last year. Finally, we have the finance and associations groups, in which there were still large proportions of high volumes.

In the public sector, where a majority of respondents transferred data about people under their administration, a majority of transfers involved small volumes, with the exception of one medical centre, three departments and one organization that reported data transfers about a very large number of people during the last five years.

Personal data transfers concerning employees generated very few large volumes, even in the private sector. The vast majority of respondents in the private sector, and almost all respondents in the public sector, transferred data about fewer than 100 employees in the last year and, even in a five-year period, only 8% of private sector respondents transferred data about 1,000 or more employees. Leading in this respect we found firms in the business and industry, associations and insurance groups and, to a lesser extent, in the fields of tourism and computer services. In the public sector, data transfers about employees still affected a low volume of people. Only 10% of respondents (N=5) transferred data about more than 100 employees during the last year, and only one organization reported transfers about more than 500 employees over a five-year period. The largest volumes were essentially found in the field of education.

Transfers of data about persons "other" than clients or employees were effected by a low proportion of respondents; paradoxically, the proportion was higher in the public sector with 18% of respondents. We would note only that the number of people affected by such data was minimal in a great majority of cases. In total, only six respondents reported having transferred data about more than 1,000 people during the last year. Because this number is so small, we cannot validly talk in terms of percentages. We see these as unique cases about which not much can be said because we do not know what people are affected by these transfers. In the private sector, respondents in all groups disclosed data to transferees abroad about other persons, but there were relatively few who did so. While more of these were found in the business and industry (five), associations (three) and miscellaneous services (three) groups, they were not necessarily the source of large-volume transfers. Only one direct marketing firm transferred data about 500,000 "others" during the last year.

The "volume of transfers" variable certainly contributes the most to understanding the issues inherent in transborder data flows. It is of even greater assistance when it is analyzed in terms of the categories of persons who are the subjects of these transfers. It is this dual perspective that will allow us to pursue our analysis of the other variables in a clear and directed manner.

5 Nature of the data

5.1 *Determination of the nature of the data*

We will now consider a question of importance to the government, given that the primary objective of this study as identified in the call for a proposal was to determine the nature of the data transferred abroad. To this end, the government prepared a list of the data relating to identifiable individuals to be covered by the study. Other items were added to these categories in order to cover the main types of data that may be disclosed to transferees abroad.

The issue was set out in question 7 of the questionnaire as follows: "Among the following information items, please indicate those which you transfer abroad: (Please check all possible answers)". This was followed by a list of 40 types of personal data from which we asked respondents to indicate all the items that they transferred abroad. For purposes of description and analysis, we subdivided these 40 types of information into nine sections dealing in turn with identifiers, socio-economic status, state of health, physical characteristics, legal history, and memberships and affiliations of, applications by, and opinions of, the person concerned.

We realized that however exhaustive this list was, it could not set out all the possibilities and so we asked respondents to identify any other types of data transferred that did not appear on the list. Accordingly, 26 respondents, including 16 in the public sector, added 18 other types of personal data that they transfer: marital status (two), social history (two), consent (one), family history (one), membership in an Indian band (one), legal proceedings (one), being able to drive a motor vehicle (two) or holding a pilot's licence (one), military status (one), competence (two), payments made or to be made (three), personal habits (one), test results (one), nature of the person's problem (one), physical marks (one), sentence to be served by the person concerned (one), relationship (one) and, finally, three other types of data that were not specified. The figures in parentheses indicate the number of respondents who reported disclosing each type of data. These figures show that these were isolated cases and that the list that we proposed to respondents covered the most common possibilities.

5.2 *Number of responses*

Upon compiling the results, we found that the 373 respondents reported a total of 3,759 types of data transferred, or an average of 10 types of data per respondent. These figures included 2,097 responses from the public sector (993%) and 1,662 for the private sector (1025%). However, we cannot rely on this average without the risk of biasing our results. Some categories of respondents clearly transfer very few items of information, others generally transfer a larger number, and some others checked off nearly all the possibilities. This suggests that, overall, they may transfer all these data either about a single person or because the data they transfer vary with the request or the purpose of transfer.

We do not believe that it would be useful in analyzing these figures to present the results for each of the 40 types of information listed, or to do a systematic comparison of the results in each sector. This sort of analysis would add little to what we can see from the results as we have grouped them. We will comment on some of the results, taken in isolation or grouped, because they have similar features, but these comments will be of limited use because the disclosure of specific data may have different meaning or impact depending on the context in which the data were transferred. The only way to do such a detailed analysis would be to conduct in-depth interviews.

The responses are cumulative, covering all data transfers effected by each respondent and, accordingly, all transferees and all purposes are combined. We could not tell what is regularly or occasionally transferred. Nor is there a cross-tabulation or more thorough study of the responses that would allow us to make all the detailed comments that would be required if we were to claim to have a picture of all the various possibilities. We will, therefore, analyze the responses to this question with all these reservations in mind.

The following tables are subdivided by category of data. The percentages given in parentheses in the table are calculated in relation to the maximum number of respondents, expressing the percentage of respondents who reported transferring the data referred to in the category headings. When there was no response, it was interpreted as a negative response.

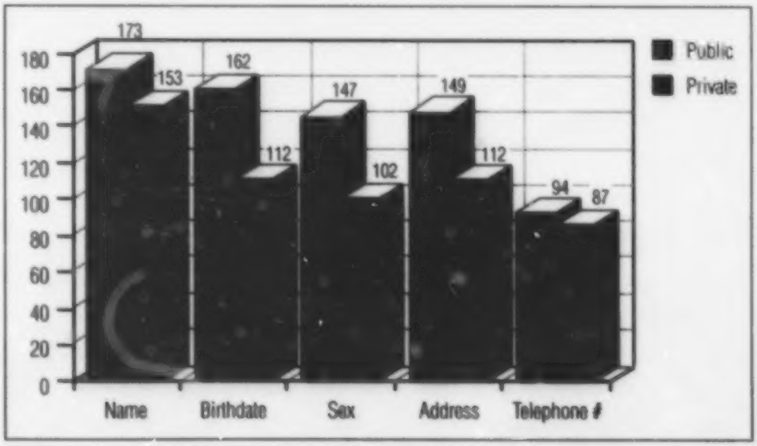
5.3 *The major identifiers*

The figures for the main types of data likely to be used as identifiers are set out in groups in Table 5-1 and illustrated in Graphic 5-1.

Table 5-1
The major identifiers

Nature of the date	Overall (%)	Public (%)	Private (%)
Family and given names	326 (87.4)	173 (82.0)	153 (94.4)
Date of birth	274 (73.5)	162 (76.8)	112 (69.1)
Sex	249 (66.8)	147 (69.7)	102 (63.0)
Address	261 (70.0)	149 (70.6)	112 (69.1)
Telephone number	181 (48.5)	94 (44.5)	87 (53.7)

Graphic 5-1
The major identifiers



Clearly, the family and given names of the persons who were the subjects of the transfers were transmitted by the largest number of respondents, although not all of them did so as we might have expected. The highest proportion of respondents who did not transfer these data was found in the public sector as a whole. It may be that the persons could have been identified by other data such as identification numbers.

The date of birth is indisputably a key information item that a very large majority of respondents report transferring abroad: 76.8% of respondents in the public sector and 69.1% in the private sector. It must also be acknowledged that this information item may, in some cases, be relevant for purposes other than identifying the respondent. The date of birth also shows a person's age, which may have been a criterion used in making certain kinds of decisions.

The same is true for people's sex, an information item transmitted by 69.7% of public sector respondents and 63% of private sector respondents. These data, together with place of birth and father's and mother's names, may be a reliable way of verifying a person's identity. All these reasons were certainly factors in explaining why a majority of respondents in all groups of firms or organizations, with the exception of finance, disclosed these data to transferees abroad.

Address and telephone number, which are generally seen with the person's name as primary identifiers, did not seem to be the only things used in this role in data transfers to destinations abroad. Although address was still an identifier of first choice, with about 70% of respondents transferring this information, telephone number was, on the other hand, transmitted by fewer than half of our respondents. This may be explained in part by the fact that this information may not have been very useful to a foreign transferee and also because this datum may be changed frequently and be of little validity in processing a file.

5.4 *Identification numbers*

A large proportion of respondents reported that they transferred other information that is used as identifiers. First, there are three numbers issued for administrative purposes by government organizations. They are, in order of importance, the social insurance number, health insurance number and driver's licence number. There follows another unspecified number, which 12.3% of respondents reported transferring. It may be a file number or an account or credit card number.

Table 5-2
Identification numbers

Nature of data	Overall (%)	Public (%)	Private (%)
Social insurance number	132 (35.4)	64 (30.3)	68 (42.0)
Driver's licence number	31 (8.3)	16 (7.6)	15 (9.3)
Health insurance number	90 (24.1)	61 (28.9)	29 (17.9)
Other number	46 (12.3)	31 (14.7)	15 (9.3)

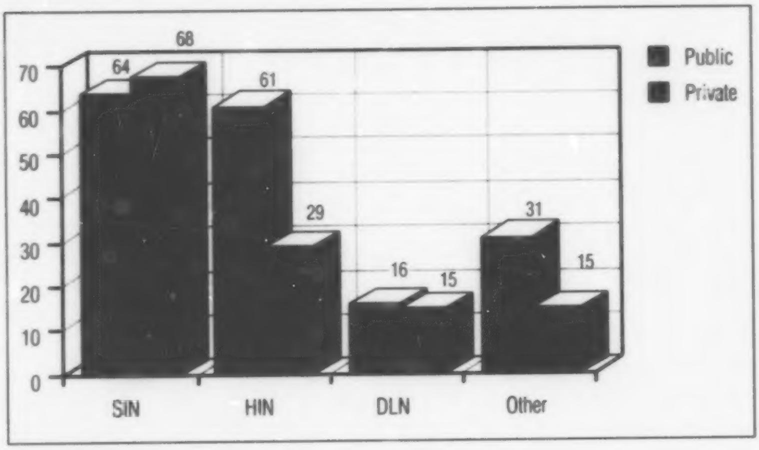
While 42% of private sector respondents reported transferring the social insurance number, only 30% of public organizations did so. This figure may be surprising at first glance but it must be recalled that the highest proportion of respondents who transferred data about their employees and for personnel management purposes was found in the private sector. This is a number that employers must have for source deductions and for income tax returns. As well, this group of firms, in which a high proportion of respondents transferred data about their employees, is mainly responsible for transferring this number. On the other hand, it is surprising to note that 43.9% of the organizations in the government group reported transferring this number, when fewer than one quarter of these organizations transferred data about their employees.

A number of private firms (17.9%) and public organizations (28.9%) disclosed the health insurance number. The reasons for transferring this number are easy to identify for health services organizations (46%) and for insurers (28%) or tourism firms (30%). On the other hand, we wonder why organizations in the government group (22%), education (16.4%) or computer service firms (25%), to name but a few, would disclose this number to transferees outside Canada.

The same question arises with respect to the driver's licence number, which firms or organizations in all fields, except communications, transfer outside Canada. No doubt some respondents have a tendency to use the largest possible number of identifiers without necessarily having any valid reason for doing so.

Graphic 5-2 illustrates the relative importance of these identifiers in data exported from Canada.

Graphic 5-2
Identification numbers



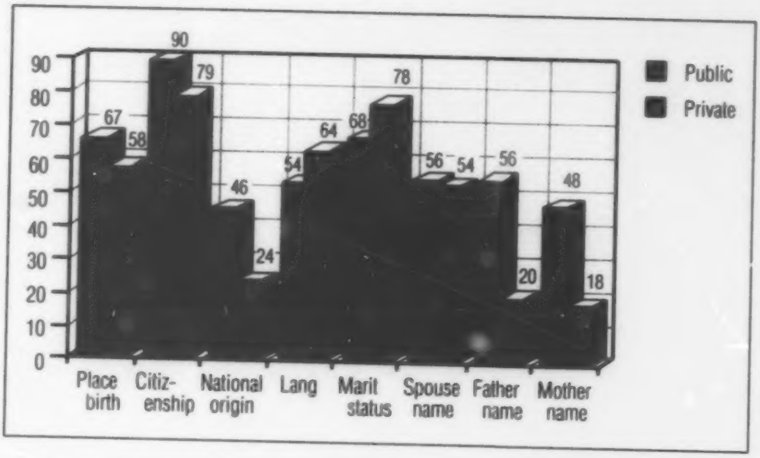
5.5 *Other identifiers*

There are eight other types of data that may be used along with other data to verify a person's identity, or may alone be the sole identifier needed by the exporter and transferee to transfer the data. They may, of course, also be transmitted for other purposes. Place of birth, citizenship and national origin, as well as the person's language of communication, may be transmitted to facilitate identifying the person as well as to indicate his or her national, ethnic or linguistic origin. The person's marital status, spouse's name and father's and mother's names may also assist in identifying him or her and can also be used for other purposes. Table 5-3 and Graphic 5-3 show the figures for the responses for these kinds of data.

Table 5-3
Other identifiers

Nature of data	Overall (%)	Public (%)	Private (%)
Place of birth	125 (33.5)	67 (31.8)	58 (35.8)
Citizenship	169 (45.3)	90 (42.7)	79 (48.8)
National origin	70 (18.8)	46 (21.8)	24 (14.8)
Language of communication	118 (31.6)	54 (25.6)	64 (39.5)
Marital status	146 (39.1)	68 (32.2)	78 (48.1)
Name of spouse	110 (29.5)	56 (26.5)	54 (33.3)
Father's name	76 (20.4)	56 (26.5)	20 (12.3)
Mother's name	66 (17.7)	48 (22.7)	18 (11.1)

Graphic 5-3
Other identifiers



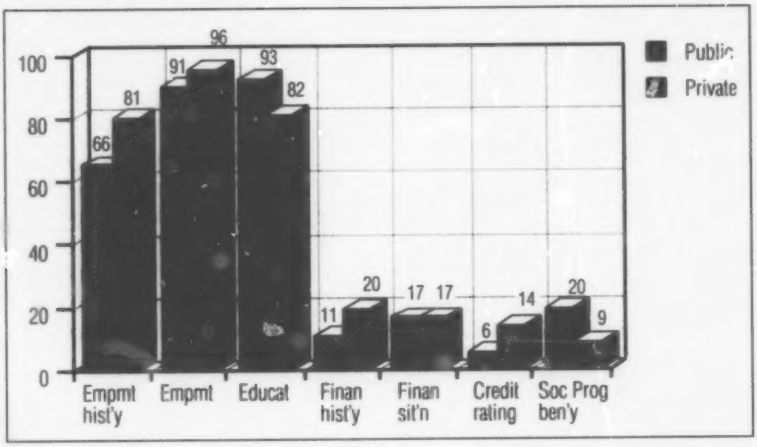
5.6 *Socio-economic status*

Data transfers about people's socio-economic status are compiled and illustrated in Table 5-4 and Graphic 5-4.

Table 5-4
Socio-economic status

Nature of data	Overall (%)	Public (%)	Private (%)
Employment history	147 (39.4)	66 (31.3)	81 (50.0)
Employment information	187 (50.1)	91 (43.1)	96 (59.3)
Education, diplomas	175 (46.9)	93 (44.1)	82 (50.6)
Financial history	31 (8.3)	11 (5.2)	20 (12.3)
Financial situation	34 (9.1)	17 (8.1)	17 (10.5)
Credit rating	20 (5.4)	6 (2.8)	14 (8.6)
Social program beneficiary	29 (7.8)	20 (9.5)	9 (5.6)

Graphic 5-4
Socio-economic status



Data about a person's employment status are transferred abroad by a large number of respondents, as shown by the figures set out in Table 5-4. More than half of the private sector respondents and more than a third of public organizations transferred data about people's employment history, employment and education.

A significant proportion of firms in all categories transferred this type of data. The exception was the finance group in which fewer than a quarter of respondents reported doing so, corresponding exactly to the proportion of respondents in this group who transferred data about their employees. Obviously there are high percentages in the groups in which a majority of respondents transfer data about their employees. In the public sector, a slightly lower proportion of respondents transmitted these data than did organizations that transmitted data about their employees. There is one exception: considerably fewer organizations in the government group transferred this information than transferred data about their employees.

A very low percentage of respondents in both the public and private sectors transferred data about people's financial situation, including financial history (5.2% and 12.3%), financial situation (8.1% and 10.5%) and credit rating (2.8% and 8.6%). In the private sector, the finance group had the highest proportion of respondents who transferred such data: 35% for financial history, 23.5% for financial situation and 29% for credit rating. These figures are hardly surprising. We note, however, that 30% of the services firms and 16% of insurers disclosed financial history.

It is important to note the fact that public organizations, particularly in the government group (22%), disclosed information about financial history and financial situation. Strangely, six organizations in the three main public sector groups (excluding the municipal group) reported disclosing people's credit rating to transferees outside Canada. We should question this practice, which is, at first glance, surprising.

5.7 *Health*

Information about health has for a long time been one of the main issues for people concerned about the protection of privacy and for people working in the medical field. For this reason, we consider it important to examine in isolation the figures on the various kinds of data relating to this issue.

Table 5-5
Health

Nature of data	Overall (%)	Public (%)	Private (%)
Medical history	119 (31.9)	89 (42.2)	30 (18.5)
Psychological tests	46 (12.3)	34 (16.2)	12 (7.4)
State of health	84 (22.5)	57 (27)	27 (16.7)

The highest proportion of respondents who transferred health data was in the public sector: medical history (42.2% compared to 18.5% in the private sector), state of health (27% compared to 16.7%) and results of psychological tests (16.2% compared to 7.4%). These data were transferred primarily by organizations in the health and social service group, three quarters of which transferred medical histories and almost half of which transferred data on general state of health. We should, on the other hand, ask why so many other public organizations outside the health services system also transferred people's medical histories (22 organizations) or data on their state of health (17 organizations).

In the private sector, we are not surprised to find that more than half of insurers transferred people's medical histories and that 40% transmitted data on state of health. What is surprising, on the other hand, is that the medical history was disclosed to transferees abroad by more than 30% of associations and tourism firms and that more than 40% of associations transferred data on people's state of health.

5.8 *Physical characteristics*

We have grouped together three more intimate types of data that identify people by their physical characteristics: photographs, fingerprints and blood group. Given the specific nature of these data, clearly a tiny minority of respondents disclosed them to transferees abroad, from 3% to 15%, as shown by the figures in Table 5-6.

Table 5-6
Physical characteristics

Nature of data	Overall (%)	Public (%)	Private (%)
Photograph	51 (13.7)	26 (12.3)	25 (15.4)
Fingerprints	13 (3.5)	8 (3.8)	5 (3.1)
Blood groups	44 (11.8)	33 (15.6)	11 (6.8)

Fingerprints were the subject of the smallest number of data transfers. These figures cannot be discussed in percentage terms. We note only that two associations, one industry, one professional services firm and one miscellaneous services firm disclosed this information while, in the public sector, eight organizations in all groups did so. In the municipal field, these may be police bodies, but we should ask what organizations in the other groups could be justified in disclosing fingerprints.

Finance and computer services were the only groups in which no firms disclosed photographs. The highest proportions of respondents who transferred this item were found in the associations, communications and tourism groups.

We might ask what firms or organizations could be justified in disclosing blood group, apart from certain insurers and health service organizations. Nonetheless, there was at least one respondent in each sector who transmitted this information, except in communications, computer services and miscellaneous services.

5.9 Legal history

Again, a low proportion of respondents (i.e., between 3% and 8%) disclosed data about legal history. Finance, computer services and professional services were the only groups in which no respondent transferred data on criminal or penal records. About 10% of respondents in all the other private sector groups reported disclosing such data. In the public sector, nearly 30% of organizations in the government group did so, 20% in the municipal group and 1% in the others. This is not many, but we must ask what organization in health services or education might have and transmit this information.

Table 5-7
Legal history

Nature of data	Overall (%)	Public (%)	Private (%)
Criminal history	27 (7.2)	16 (7.6)	11 (6.8)
Civil judicial background	11 (2.9)	6 (2.8)	5 (3.1)

5.10 *Memberships and affiliations*

Data relating to memberships and affiliations may be "sensitive", depending on the reasons for which it is transferred and who the transferees are. In our questionnaire, we identified four categories of memberships: political affiliation, union membership, religious affiliation and other association membership. We have set out the results in Table 5-8.

Table 5-8
Membership and affiliations

Nature of data	Overall (%)	Public (%)	Private (%)
Political affiliation	2 (0.5)	1 (0.5)	1 (0.6)
Union membership	16 (4.3)	6 (2.8)	10 (6.2)
Religious affiliation	36 (9.7)	21 (10.0)	15 (9.3)
Other association membership	26 (7)	12 (5.7)	14 (8.6)

These figures show that there is no significant difference between the public and private sectors. In order of importance, the information items in question were: religious affiliation (9.7% and 10%), association membership (5.7% and 8.6%), union membership (2.8% and 6.2%) and political affiliation (0.5% and 0.5%).

Political affiliation truly stands out with two respondents who transmit this type of data: one government organization and one communications firm. The highest percentage of respondents who disclosed the other three types of data was all in the associations sector, the reason being that membership in the association is the very basis of the activity of these organizations. Thus 11 out of 15 respondents who indicated religious affiliation and six of the 10 who indicated union membership as types of data transferred, are associations. Finally, we found respondents who disclosed association membership in six public sector groups.

5.11 *Applications, correspondence and opinions*

A low percentage of respondents transferred personal data relating to personal initiatives and opinions. These may be applications by a person to an organization or firm (for example, by making a complaint or request) or correspondence by a person with an organization or firm. They may also involve the opinions of the person concerned, which might be found in correspondence, for example, or the opinions of others about the person, as such or in the form of evaluations or ratings (for example, credit ratings, analyzed in section 5.4). Table 5-9 sets out the results of the survey with respect to disclosure of such applications or opinions in transborder data transfers.

Table 5-9
Applications and opinions

Nature of data	Overall (%)	Public (%)	Private (%)
Applications by person	49 (13.1)	24 (11.4)	25 (15.4)
Correspondence of person	32 (8.6)	14 (6.6)	18 (11.1)
Person's opinions	30 (8.0)	17 (8.1)	13 (8.0)
Opinions of others	54 (14.5)	31 (14.7)	23 (14.2)

Overall, there is no remarkable difference between the two sectors, with the exception of correspondence and applications by the person, which were transmitted by a larger proportion of private sector respondents.

For the last three types of data, communications firms dominate. This situation may be explained by the fact that a significant proportion of the respondents in this group is composed of publishers whose business is the realm of ideas.

For people's correspondence, the highest percentage of respondents who transmitted such data was found among the associations (23.1%), insurers (12%) and finance (11.8%) groups. Services firms (20%) and associations (11.5%) were the main exporters of the opinions of the person who was the subject of the transfers.

Only one group of respondents, those in finance, did not disclose other people's opinions of the person. Six of the eight remaining groups show results higher than the private sector average (14.2%). They are, in order, services firms (30%), transportation and tourism firms (20%), associations (19.2%), computer services firms (16.7%) and professional services firms (14.3%). In the public sector, there were no such transfers by municipal organizations, but those in the government group were well in the lead, particularly for others' opinions (29.3%) and the person's correspondence (17.1%).

To summarize, relatively few private firms or public organizations disclosed these types of data. However, because this information may have been "sensitive", it was important to know who was transmitting such data and for what purposes. Our survey provides a basis for targeting the sensitive points.

5.12 *Summary and conclusions*

It would be presumptuous to try to summarize an analysis dealing with data that are so sparse and often insignificant and which, in the circumstances, can only be incomplete and sometimes even superficial. Our analysis of the responses relating to the nature of the data disclosed to transferees abroad was actually considerably limited by the fact that respondents reported all the data they may transfer, without being able to specify the circumstances in which they did so: the frequency, the purpose, the transferee and the number of people with respect to whom they normally do so.

These are cumulative results, which reflect only one aspect of the situation and which do not allow for the detailed analysis that cross-tabulating with other variables would permit. But it would also be unrealistic to think that one study carried out on these terms would provide us with all the necessary data for a complete and detailed analysis. However, the results obtained provide us with an outline of the scope of this phenomenon, an indication that anything may be transfe[illegible]. There is no information that is neutral or dangerous in itself since such an assessment depends on various factors.

For the purposes of our analysis, we grouped various types of data under nine headings exhibiting certain common features. This approach made it possible to discern significant trends for each sector or for certain groups of subsectors. We note immediately that each respondent reported on average 10 types of data that it transferred abroad, this figure being slightly lower for the public sector (9.93) than for the private sector (10.25).

The data that we grouped under the identifier headings were disclosed by a large proportion of respondents in both sectors. In first place were the traditional identifiers: family and given names, date of birth, sex, address and, to a lesser extent, telephone number, marital status and spouse's name.

Next were various numbers issued by the government for administrative purposes. The social insurance number was most frequently disclosed, especially in the private sector where a majority of respondents transmit data about their employees. The health insurance number was disclosed mainly by health service organizations and insurers and tourism firms, which was predictable. However, disclosure of this number by a large number of other organizations or firms remains inexplicable. Other data that may be used as supplementary identifiers were transmitted by fewer than a quarter of respondents.

Data on people's employment history, experience and education were disclosed by a significant proportion of respondents, particularly in the private sector where a large majority of firms transferred data about their employees. Few respondents disclosed data on people's financial situation. This may be explained by the fact that few firms in the finance sector responded to our questionnaire.

The highest proportion of respondents who disclosed data on people's state of health was found in the public sector and among insurers. Physical characteristics, such as fingerprints and blood group, as well as legal histories, were transferred mainly by public organizations.

However, there were respondents who disclosed these data in almost all groups, a fact that we find perplexing.

Some types of data that may be sensitive, such as memberships and affiliations, applications and opinions, were disclosed by a very small minority of respondents in both sectors. Certain groups of subsectors dominate in this area: for memberships and affiliations, associations and the government group; and for opinions, the communications group, which leads in the private sector while government again dominates the public sector.

These results allow us to identify certain core groups where either large amounts of personal data, or data that might be "sensitive", depending on the use made of it, were disclosed. However, this does not necessarily help us to understand what the justification might be for the transfer by some organizations or firms of data that at first glance seem to bear little relation to their principal activities.

Despite these limitations, we can nonetheless draw one general conclusion based on our analysis of these results: anything may be disclosed, even in the context of transborder transfers. Some categories of respondents show all the symptoms of a prodigal approach to their data. It seemed difficult for them to select the pertinent data, unless they were themselves subjects of demands by their transferees. In either case, the question of the relevance of the data disclosed is more important today than ever before.

6 Methods of transfer

We asked respondents to indicate the method by which they usually disclose data to transferees abroad by stating all methods used and, if possible, identifying the proportion of data transferred by each method. The question was formulated as follows:

> *8. In which of the following forms do you usually transfer your data?*
> *(Please check √ all possible answers or give percentage (%) volumes if available):*
>
> *a) Communication of all information held on individuals* ____
> *b) Communication of a series of information items drawn from a series of individual files* ____
> *c) Communication of all information held on an individual* ____
> *d) Communication of a few items of information drawn from an individual's file* ____

6.1 Rate of response

As shown by the figures in Table 6-1, respondents as a whole provided 426 responses to this question, amounting to a 114.2% response rate overall. The rate was 114.6% in the public sector and 113.5% in the private sector.

We asked respondents to indicate, if possible, the proportion in which they use each of the methods of transfer listed. Fewer than 10% of the responses provided such percentages, except for respondents who disclose all information held on all individuals. Although this was a small number of respondents (six), they were concentrated in the public sector. We can, therefore, discuss these figures when we deal with the results in this sector, although we cannot interpret them as reflecting a trend.

6.2 *Analysis of results*

1. If we read the figures in Table 6-1 and illustrated in Graphic 6-1, we find that there is really no cleavage between the two sectors in terms of the method of disclosure used by respondents. In both cases, a few items of information drawn from an individual's file were disclosed in a majority of transfers effected by respondents. We found the highest percentage of transfers using this method in the public sector with 87.2% of respondents, while fewer than 65% of private sector respondents disclosed data in this way.

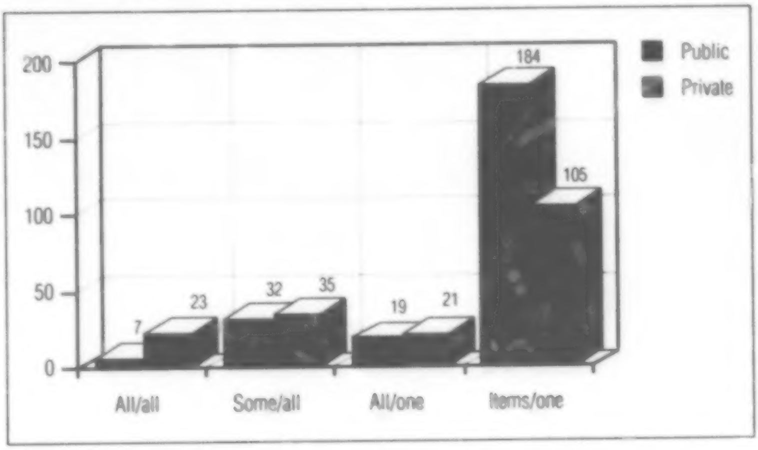
   Next, but very far behind, are cases in which respondents disclosed a series of information items drawn from a series of individual files, 18% of all responses. Transmission of a list of the names and identifying data of people selected because they belong to a target population would be included in this category.

   While the percentages of respondents who reported disclosing all information held on an individual or all information held on all individuals were relatively low, nonetheless a relatively large number of respondents reported doing so. We should pay particular attention to this fact, something we will do in analyzing the results for each method of disclosure, by sector.

Table 6-1
Methods of disclosure

Methods	**Overall (%)**	**Public (%)**	**Private (%)**
All info on all individuals	30 (8.0)	7 (3.3)	23 (14.2)
Series of info items drawn from a series of files	67 (18.0)	32 (15.2)	35 (21.6)
All info on an individual	40 (10.7)	19 (9.0)	21 (13.0)
A few items on an individual	289 (77.5)	184 (87.2)	105 (64.8)
Total: Responses/respondents	426/373	242/211	184/162

Graphic 6-1
Methods of transfer



2. We will deal with each of the methods of disclosure in the order in which they were used by respondents as a whole. First is disclosure of certain data on an individual. We have seen that more than 87% of public organizations used this method of disclosure. When we considered the results for each group that makes up this sector, we got relatively uniform figures. The respondents who used this method varied from 80% for the municipal group to 89% for the education group. We would note that 14 of the 184 organizations that used this method specified the proportion in which they do so. Of these, nine respondents report that 100% of the data they transferred abroad was disclosed in this manner. The percentage of use varied from 1% to 79% for three organizations in the health and social services group and one organization in the government group.

   In the private sector, 64.8% of firms used this method of disclosure. Here again we found that results were consistent for a majority of groups. For seven of them, the percentages varied from 60% to 68%. The tourism group and professionals group stand out. At one extreme, 30% of respondents in the first group used this method; at the other, it was used by 78.6% of respondents in the second group. Of the 105 firms concerned, 12 specified the proportion in which they used this method to disclose data. For four of them (two in insurance, one in business and industry, one in computer services) this was the only method they used while for the eight others, no method predominated.

3. Disclosure of a series of information items drawn from a series of files was the method used by 15.2% of public organizations. The two groups that use this method to the greatest extent are education with 19.2% and health and social services with 14.9%. On the other

hand, only 12.2% of organizations in the government group and 10% of municipal organizations used this method.

This method of disclosure was used by a larger proportion of private firms: 26%. The results were consistent for a majority of groups, tourism firms (40%) and associations (30.8%) heading the list and firms in the finance group bringing up the rear with 11.8% of respondents using this method to disclose data.

4. Next comes disclosure of all information held on all individuals. For all practical purposes, it is pointless to compare the situation among the nine groups with such small figures. We note only that in some groups, primarily the finance, professionals and insurance groups, few or no firms reported using this method to disclose data. On the other hand, 40% of the transportation and tourism firms and the miscellaneous services firms used this method of disclosure.

   In the public sector, the highest percentage of respondents who used this method were found in the government group with 19.5% of respondents, two of which specify that this was the only method they use to transfer data abroad. Next are organizations in education and in the social services group with 9.1% and 5.5% of respondents, respectively, using this method. There is nothing to indicate whether this was a common or occasional practice.

5. Disclosure of all information held on all individuals was used by 14.2% of private firms. As these 23 respondents were distributed throughout the nine groups of firms, it would be futile to play with percentages involving such low numbers. We note only that, in absolute figures, the insurance group dominated with five respondents, one of which specified that this method was used for 100% of the data it disclosed while, in percentage terms, firms in the tourism group had the highest rate of use of this method of disclosure, 30% of respondents.

   Although only a low percentage of public organizations (3.3%) use this method to disclose data, it would be important to know who they are, to whom they transfer these data and, particularly, what the purposes are for disclosing data to transferees abroad using this method.

6.3 *Summary and conclusions*

We find very little variation among the groups in each sector, particularly for the two most commonly used methods of disclosure: a few items on an individual and a series of items from a series of files.

Disclosure of a few items on an individual was more widely used in the public sector (87.2% of respondents) than in the private sector. In the public sector, the figures varied little from one group to another while in the private sector two groups stand out: transportation and tourism with 30% and professionals with 78.6%.

Disclosure of a series of information items from a series of files was second for both sectors, with 15.2% and 21.6% of respondents. Well in the lead were tourism or transportation firms (40%) and associations (30.8%).

The two other methods of disclosure involving all information on one or more individuals were used by too small a number of respondents to be able to analyze the figures in percentage terms. We note only the groups of firms or organizations that predominate: transportation and tourism firms and organizations in the government group, in which 40% and 19.5% of respondents reported disclosing all information held on an individual. Transmission of all data on all individuals was the method used by a small number of respondents in all groups of firms, only the insurance group standing out with five respondents.

It appears from this brief analysis that the most widely used method of disclosure in the groups making up the two sectors, as a whole, was disclosure of a few information items on an individual.

7 Forms of disclosure

We defined five forms of disclosure, asking respondents to identify those that they normally use to disclose data to transferees abroad by checking off all possible answers and indicating, if possible, the proportion in which they use each of these forms. The question set out in point 9 of the questionnaire read as follows:

> 9. *Which means of communication are generally used for your personal data transfers?*
> *(Please check √ all possible answers or give percentage (%) volumes if available):*
>
> *a) Magnetic (tape, discs, etc ...)* ____
> *b) Telecommunications*
> *(access to your data available from abroad)* ____
> *c) Telecommunications*
> *(transfer by your services)* ____
> *d) Hard copy (including fax)* ____
> *e) Telephone (verbal)* ____

7.1 Rate of response

Respondents provided 593 responses for all sectors as a whole, for an average of 1.59 responses per respondent. The average response was slightly higher in the private sector, with 1.69 compared to 1.52 in the public sector, indicating that, on average, private firms disclose data to transferees abroad in a wider variety of forms than do public organizations.

As for the preceding variables, few respondents stated the proportion in which they used the various forms of disclosure. We counted only

47 cases in which percentage responses were given, representing 7.9% of the responses received. The private sector led with 9.5% compared to 6.6% for the public sector.

7.2 *Analysis of responses*

1. The figures set out in Table 7-1 speak eloquently. Traditional forms of disclosure were used by a large majority in transferring data abroad. The highest proportion of respondents who used hard copy, including telecopier (fax), to transfer data was found in the public sector (89%), compared to 76.5% of private firms using this form. On the other hand, the proportion of private firms that transferred data by telephone was slightly higher (44.4%) than in the public sector (40.3%).

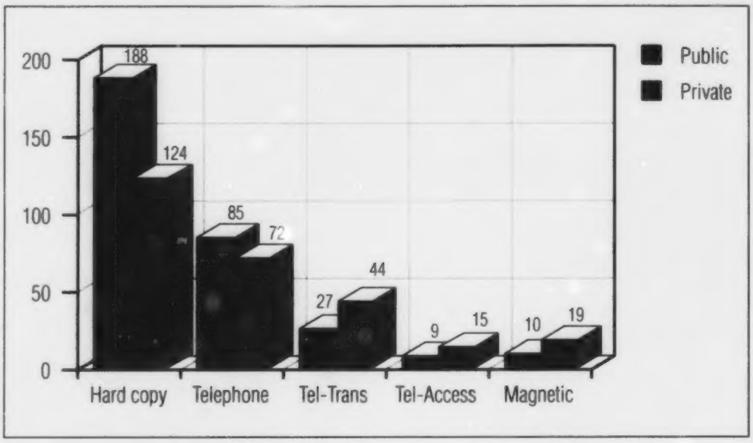
The highest proportion of respondents who used telecommunications and magnetic media to disclose data to transferees abroad was found in the private sector. In total, 36.5% of them reported using telecommunications (access and transfer) and 11.7% magnetic media, compared to public sector figures of 17.1% and 4.7%, respectively.

Table 7-1 and Graphic 7-1 set out these results.

Table 7-1
Form of communication

Type of media	Overall (%)	Public (%)	Private (%)
Magnetic	29 (7.8)	10 (4.7)	19 (11.7)
Telecommunications - access	24 (6.4)	9 (4.3)	15 (9.3)
Telecommunications - transfer	71 (19.0)	27 (12.8)	44 (27.2)
Hard copy	312 (83.6)	188 (89.1)	124 (76.5)
Telephone	157 (42.1)	85 (40.3)	72 (44.4)
Total: Responses/respondents	593/373	319/211	274/162

Graphic 7-1
Forms of disclosure



2. We will now determine whether we can find variations or consistencies among the various groups in each sector in terms of their use of each of the forms of disclosure. We will deal with each form in order of importance.

Although a very large majority of respondents reported disclosing data in manuscript form, we found that the situation was not uniform for all groups in the private sector. More than 905 of the firms in the associations, tourism, professionals and miscellaneous services groups transferred data in hard copy form, while 80% and 87.1% of the services and communications firms used this form. On the other hand, manuscript was used much less frequently in three other groups of firms: insurance with 60%, computer services with 58% and finance with 41.2%.

We also found a very high degree of homogeneity in the responses given by respondents in the four public sector groups. More than 88% of organizations in the three largest groups used hard copy to disclose information to transferees abroad, only the municipal group falling behind somewhat with a rate of 80%.

The situation in the private sector with respect to use of the telephone as a medium of disclosure was in many ways similar to the situation we noted with respect to the use of hard copy. We found an above-average rate of use in the same groups: services (90%), tourism (70%), professionals (57.1%) and associations (57.6%). Again, firms in the insurance and finance groups avoided this form of disclosure, with rates of use of 12% and 29.4% respectively.

This time the situation was more diversified in the public sector: only 30.1% and 36.7% of the organizations involved in education and health and social services used the telephone to transfer data, while more than 60% of the municipal and government organizations did so.

While the results with respect to the use of forms of disclosure relying on new technologies were not the complete opposite of what we found for the more traditional forms, they did indicate a certain reversal in the situation. For cases where data were transferred using telecommunications, the highest proportions were found in the groups that had low rates of use for manuscript and telephone: insurance with 48% and firms in the finance group with 35.5%. These two categories of firms were the furthest above the average for the private sector (27.2%). Another variation found was that only 10% of firms in the communications and miscellaneous services groups used this form of communication.

With respect to direct access using telecommunications to data held by firms, we would note that miscellaneous services and communications were the only groups where no firm reported disclosing data in this manner. All other types of firms used this form of disclosure in proportions approaching the low average of 9.3% for the private sector.

In the public sector, we cannot compare the situation in each group because the number of respondents is too small. We note only that from one to three organizations per group used this form of disclosure. It would be interesting to know who may have had access to these data and for what purposes.

The highest proportion of respondents who reported using magnetic media to disclose data was found in the tourism, computer services and services groups; however, this percentage did not exceed 33% in any case. Only in the associations group did no firm use this form of disclosure.

In the public sector, the highest percentage of respondents who used this form of disclosure was found in the health and social services (6.9%) and government (14.9%) groups. However, it should be noted that a total of only 10 organizations reported using magnetic media.

7.3 *Results of earlier studies*

Studies done over an interval of several years by various organizations also indicate that the traditional forms of disclosure were most widely used in transferring data. For example, the 1983 study by the Intergovernmental Bureau for Informatics in Rome showed that a majority of respondents used telephone and telex to transfer data outside national borders, while only 29% of respondents used computers for this purpose. However, we should note that Third World countries made up 80% of the sample. When we consider the figures for the European and North American countries, we found that more than

60% of respondents reported using computers to send data abroad, something very different from the results of our study.

On the other hand, a more recent study completed in 1988 by EDI Research Inc indicates that 75% of data transfers between firms were effected on paper media, 16% were oral and only 10% of exchanges were effected electronically. It should be noted, however, that these studies did not deal exclusively with personal data.

While the results of our study show that the traditional forms of disclosure were widely used to transfer data, they also show that these forms were used concurrently with electronic forms by a large proportion of respondents, primarily in the private sector.

7.4 *Summary and conclusions*

Hard copy was the main form of disclosure used overall by the firms and organizations that participated in our survey. On the other hand, forms of disclosure relying on new technologies were used by a minority of public sector respondents. The fact that a majority of the transfers from this sector relate to one individual at a time and that the data transferred were sent to multiple destinations was, of course, a factor in explaining why the traditional forms of disclosure were still widely used. In the private sector, a much larger proportion of respondents used magnetic media and telecommunications to send their data abroad; however, this sector did not in any way abandon the traditional forms of transfer, with the exception of firms in the finance and insurance groups.

8 Protection and guarantees

In the final question in our survey we dealt with the protection and guarantees enjoyed by individuals who are the subjects of the data transferred abroad. For this purpose, we outlined the main forms of protection and guarantees accorded by most privacy protection legislation.

8.1 *Protection*

Points 10a) and b) of the questionnaire dealt with the protection and guarantees enjoyed by individuals who are the subjects of the data transferred abroad:

10. When you transfer personal data to a foreign destination:

a) Are the affected individuals informed of these communications?
always ___ in certain cases ___ never ___

b) Can these individuals:
(if positive, please check √)
- *obtain access abroad to the transferred data?* ___
- *have this data corrected abroad, if there is cause?* ___

In Table 8-1 we grouped the results for three types of protection generally accorded by privacy protection legislation: informing the person that data concerning him or her are being disclosed, access to data transferred about him or her, opportunity to make corrections if there is cause.

Table 8-1
Notice, access and right of correction by data subjects

Protection	Overall (%)	Public (%)	Private (%)
INFORMING INDIVIDUALS			
Always	299 (80.2)	173 (82.0)	126 (77.6)
In certain cases	39 (10.5)	21 (10.0)	18 (11.1)
Never	19 (5.1)	9 (4.3)	10 (6.2)
No response	16 (4.3)	8 (3.8)	8 (4.9)
ACCESS TO DATA			
Yes	182 (48.4)	92 (43.6)	90 (55.6)
No response	191 (51.2)	119 (56.4)	72 (44.4)
OPPORTUNITY TO CORRECT			
Yes	182 (48.4)	81 (38.4)	101 (62.3)
No response	191 (51.2)	130 (61.6)	61 (37.7)

1. A very high proportion of people responded to the first part of the question, more than 95% of respondents as a whole. We cannot determine the rate of response to the other parts of the question because people were asked to respond only if their response was positive. However, there is every reason to believe that all respondents who answered the first part of the question would have continued to read it and to respond when they had a positive response to provide. Given the low rate of non-response to the first sub-question, for the purposes of our analysis we will consider a non-response as a negative response to the various sub-questions.
2. A very large majority of respondents reported that the subjects of data transfers were "always" (80.2%) or "in certain cases" (10.5%) informed of such transfers. The highest percentage of totally affirmative responses was found in the public sector. There was relative-

ly little variation among the various groups. We would, nonetheless, note that there were variations in the private sector groups: 92.3% of associations and 88% of the insurance group reported that the data subjects were always informed when data about them were transferred. The lowest percentage of firms reporting that the data subjects were "always" informed was found in the business and industry category with 64.5% of respondents, of which 25.8% reported that the individuals were informed of such transfers "in certain cases". These facts are a cause of concern when we know that a majority of firms transfer data about their employees. How can they be kept unaware of such transfers?

Some of the figures in the public sector leave us perplexed. Only 70% of the respondents in the "government" group and 50% of municipal organizations reported that the data subjects were always informed of transfers of data about them. In addition, 4.4% of respondents reported that people were never informed of such transfers, reaching a high of 30% in the municipal group. It's a good bet that, in a majority of cases, these were organizations that disclosed data about several individuals at a time. Almost all organizations in the education group always (89%) inform the data subjects of the transfers or did so in certain cases (4.1%).

It is interesting to note that some respondents stated that the individuals affected by the data transfers were not necessarily informed either because all disclosures must be authorized by the individual or because data were transferred at the request of the person concerned. The first argument for this assertion was presented mainly by representatives of health service institutions, the second mainly by educational institution respondents. We note that these are public organizations that are in some jurisdictions governed by legislation requiring them to inform the individuals of any disclosures of data about them and requiring the consent of such individuals. There is nothing of this sort in the private sector in Canada; this is why it is surprising to find that so large a majority of respondents in this sector report that people are always informed when data about them are disclosed.

3. With respect to the opportunity to obtain access to data transferred abroad, it is paradoxical to find that the lowest proportion of respondents (43.6%) who stated that data subjects have such an opportunity was found in the public sector. This percentage was even below 40% in the municipal and health service fields. In the private sector, 55.6% of respondents reported that people have access to data abroad.

   Still more paradoxical is the fact that, in the groups in which from 100% to 85% inform data subjects of disclosures, only 46% or 40% of them reported that people had access to such data abroad. Logically, we should find above-average figures for opportunity to have access to the data transferred in those groups where people are almost always informed of disclosures.

Some respondents justified not being able to respond to the question on the right of access and correction because the response depended on the law in effect in the countries of destination. This explanation was given mainly by representatives of public organizations. One representative of a provincial organization even indicated that the countries of destination probably had legislation offering protection similar to what is provided by that province's privacy and access legislation.

4. A very high percentage of private sector respondents (62.3%) reported that there was an opportunity to correct data held abroad, compared to 38.4% of public organizations.

The percentage for this response in the insurance, business and industry and professional services groups exceeded the 70% level. In insurance, we know that the Medical Information Bureau requires life insurers who use its services to inform people that data about them are being disclosed and to advise them how to proceed in order to consult their records and make corrections. In the public sector, fewer than a quarter of respondents in the health and social services group reported that people had the right to make corrections. The proportion was higher in the education (50.7%) and government (46.3%) groups.

These inconsistencies may be seen in an example. Almost all insurers inform people that information about them is being disclosed. Up to here everything is fine. Some 60% of insurers reported that people have access abroad to data transferred and 76% reported that people could make corrections to such data. Respondents in the business and industry, associations, transportation and tourism, computer services and services groups provided the same sort of response, more of them reporting that people could correct information than that they had access to the data transferred.

For the moment, the only way we can explain these inconsistencies would be that respondents did not clearly understand the question and, in responding to it, had in mind the opportunity to correct data before it was transferred abroad.

8.2 *Guarantees provided by transferees*

We set out five types of protective measures in the questionnaire. We wanted to know whether the data transferees provided guarantees that they would provide such protection, specifying the use of data transferred, the relevance of data for such uses, guarantees of the confidentiality and security of the data and, finally, limits on the time that the data disclosed may be held. The question read as follows:

10 c) Do you receive from your foreign recipients guarantees concerning:
(If positive, please check √ all possibilities)

	always	*in certain cases*
- *the eventual uses of data transferred?*	____	____
- *the relevance of data for such uses?*	____	____
- *the confidentiality of data?*	____	____
- *the security of data and communications?*	____	____
- *the time for which information will be held?*	____	____

Table 8-2
Guarantees provided by transferees

Types of guarantees	Overall (%)	Public (%)	Private (%)
AS TO USE			
Always	170 (45.6)	88 (41.7)	82 (50.6)
In certain cases	59 (15.8)	37 (17.5)	22 (13.6)
No response	144 (38.6)	86 (40.8)	58 (35.8)
AS TO RELEVANCE			
Always	166 (44.5)	89 (42.2)	77 (47.5)
In certain cases	49 (13.1)	29 (13.7)	20 (12.3)
No response	158 (42.4)	93 (44.1)	65 (40.1)
AS TO CONFIDENTIALITY			
Always	204 (54.7)	105 (49.8)	99 (61.1)
In certain cases	53 (14.2)	30 (14.2)	23 (14.2)
No response	116 (31.1)	76 (36.0)	40 (24.7)
AS TO SECURITY			
Always	135 (36.2)	58 (27.5)	77 (47.5)
In certain cases	45 (12.1)	23 (10.9)	22 (13.6)
No response	193 (51.7)	130 (61.6)	63 (38.9)
AS TO TIME			
Always	62 (16.6)	22 (10.4)	40 (24.7)
In certain cases	70 (18.8)	37 (17.5)	33 (20.4)
No response	241 (64.6)	152 (72.0)	89 (54.9)

We grouped the figures for responses to this question in Table 8-2. We included non-responses in calculating percentages, given that they may be considered as a negative response rather than as a refusal or inability to respond. If the respondent was unable to respond, we understood that this means there was no guarantee. In one case, the representative of a government organization did not respond to this question because the response was "conditional on the legislation of the countries of destination".

The first observation is that a higher percentage of respondents in the private sector reported that transferees provide guarantees for all five types of guarantee listed in our questionnaire.

The highest percentage of positive responses in both sectors came with respect to the confidentiality of the data, 66.1% for the private sector and 49.8% for the public sector. In this area, there were three leading private sector groups: insurers (84%), firms in the business and industry group (74.2%) and associations (61.5%) with figures that are above average in terms of guarantees of confidentiality always being obtained from data transferees. Professional services (42.9%) and communications (10%) firms are in the distant rear. In the latter case, these results are understandable because a large proportion of respondents are in the publishing sector. In the public sector, the situation is comparable to the average figures for the sector as a whole, with the exception of the municipal group where a very large majority of organizations did not respond.

Next come guarantees concerning the use of the data, with 50.6% in the private sector and 41.7% in the public sector, closely followed by guarantees concerning the relevance of the data disclosed for the intended use, with 47.5% for the private sector and 42.2% for the public sector.

With respect to guarantees as to the use to be made of the exported data, four private sector groups lead: firms in the finance, insurance, computer services and associations groups. In the public sector, there were no noticeable variations among the groups. Respondents in the same groups were in the first four places in terms of guarantees obtained from transferees as to the relevance of the data transferred. This time, computer services firms were in second place, well behind insurers. For both these types of guarantees, there was little difference in the figures among the public sector groups, being all close to the average for the sector. There was a higher rate of non-response, however, among organizations in the health and social services group.

Far fewer private sector respondents (27.5%) than public sector respondents (47.5%) reported that transferees gave them guarantees as to the security of these data and communications. In this respect, three groups lead the private sector: again, insurers, followed by firms in the business and industry and computer services groups. If we add respondents who obtain guarantees of security "in certain cases", associations and finance firms are close behind, along with transportation and tourism firms.

In the public sector, more than half the organizations in the government group obtained guarantees of security from transferees, always doing this "in certain cases". A large majority of other organizations did not respond to this question.

Finally, while only 10.4% of public sector respondents reported that transferees provide guarantees as to the time data is held, nearly a quarter of private firms (24.7%) reported such guarantees. Still far in the lead were insurers and computer services firms. Close behind were firms in the finance groups, where more than a third of respondents always obtained guarantees of security. Finally, a large proportion of tourism firms, businesses and industries obtained such guarantees from transferees. In the public sector, three quarters of respondents did not answer this question, indicating that, because these cannot all be failures to answer, a large proportion must be negative. Organizations in the government group were in the lead: 14.6% always obtain guarantees as to the time data are held, 31.7% doing so in certain cases.

8.3 *Summary and conclusions*

From this brief analysis of the responses to the question dealing with the protection offered to people who are the subjects of data transferred abroad and guarantees provided by transferees, we see that in a majority of cases the data disclosed are well protected and the people affected by the disclosures are rarely kept in the dark about their occurrence.

These are the conclusions inspired by the responses of the respondents as a whole, if we assume that they were given with full knowledge of the facts. Some results are surprising, because they present a positive picture of the situation, primarily with respect to the protection offered to the people concerned, particularly when the data transfers occur in the private sector. So much the better, if true, for example, that in more than 80% of cases the persons affected by the disclosures were informed of them. However, we might assume that, in some cases, respondents may have tended to respond on the basis of a widespread belief that people must be aware that data about them will be exchanged. However, there is a difference between this assumption and assuming that people will know that such data will be disclosed to transferees outside the country — a difference that some respondents might not have observed.

A summary overview of the results gives us an idea of the extent to which respondents were painting a positive picture, particularly in the private sector. The only case in which public sector respondents are in the lead is with respect to informing the individuals who were the subjects of the data transferred, where 80% of public organizations reported that people are always informed of such transfers compared to 77.6% of the private firms.

The greatest proportion of positive responses with respect to the right to have access abroad to transferred data and the right to correct it is found in the private sector, with 55.6% for access to data and 62.3% for opportunity to correct. This latter figure seems abnormally high, given that the opportunity to correct appears to be more widespread than access to the data transferred. In the private sector, insurers are in the lead for these three types of protection while, in the public sector, educational organizations provide the highest proportions of positive responses.

The responses with respect to guarantees offered by transferees indicate considerable concern on the part of a large proportion of the public organizations and, particularly, the private firms that engage in personal data transfers. This is true for the first four types of guarantees, but less so for the issue of the confidentiality of data.

These results are surprising, particularly because we know that legislation to ensure the protection of personal data, and access by people to data concerning them, exists essentially in the public sector. Accordingly, we could suggest that this fact might have helped to generate greater awareness among people in the private sector of the importance of protecting these rights and requiring guarantees from the organizations with which they exchange data. It seems that private sector respondents have also been affected by these issues.

The only similarity between the figures in each of these sectors is with respect to guarantees provided by transferees concerning the confidentiality of communications and of data transferred, this being the area in which the largest number of respondents report obtaining guarantees.

Next come guarantees concerning the use of the data and the relevance of the data for the proposed use. A larger proportion of private firms (50.6% and 47.5%) than public sector organizations (41.7% and 42.2%) always obtained such guarantees. The figures for three groups of private sector firms were above the average: insurers, computer services firms and finance. The figures for the various groups in the public sector are comparable for these two types of guarantees.

Finally, the public sector really brings up the rear in terms of guarantees concerning security and the time data will be held. Only the figures for organizations in the government group are comparable with respect to guarantees obtained as to the time data will be held.

For both these types of guarantees, the insurers group is still well in the lead, followed at a distance by computer services. Respondents in the business and industry group rank second in terms of guarantees of security, while the finance and tourism groups rank third and fourth in terms of guarantees as to the time data will be held.

9 Very large volumes of exports

After analyzing the results for each of these questions, we considered it important to give special attention to the cases of respondents who reported transfers of very large volumes of personal data. In so doing, our purpose is not express surprise that greater numbers of air carriers or banks did not report transferring very large volumes of personal data but, rather, to identify all those respondents who disclosed personal data about more than 10,000 individuals to transferees abroad or reported that the total number of individuals affected by all data about them held abroad, owing to transfers of data originating from a single respondent, exceeded 100,000 individuals. This is what we mean by large volumes.

We identified 26 respondents reporting transfers of very large volumes. Tables 9-1 and 9-2 indicate the sectors in which they originated plus the group and the subsector of each of the respondents who transferred large volumes of personal data abroad. In these tables, the figures refer to clients for the private sector and persons under the administration of organizations in the public sector. The notation (e) refers to data transferees about "employees" while (o) refers to "others".

The tables clearly show that a majority of the 26 respondents who transfer very large volumes of personal data were in the private sector (21), while only five public sector respondents transferred such large volumes abroad. In fact, the 21 transferors of very large volumes in the private sector represent 13% of the 162 respondents in that sector who reported transborder data transfers. In the public sector, the proportion barely exceeds 2% (5/211).

Table 9-1
Exporters of large volumes, public sector

Group	Subsector	1 year (10,000 +)	5 years (10,000 +)	total (100,000 +)
HEALTH/ SOC SERVICES	hospital		15,000	
GOVERNMENT	other org'n		28,000	
	department		10,000	
	department	30,100	125,300	
	department		10,690 (o)	

Table 9-2
Exporters of large volumes, private sector

Group	Subsector	1 year (10,000 +)	5 years (10,000 +)	total (100,000 +)
ASSOCIATIONS	union		20,000	
INSURANCE	insurance		40,000	
	insurance		12,000	
	insurance	10,000	50,000	
	insurance		10,000	
	insurance	40,000		
	insurance	150,000	600,000	150,000
	insurance		20,000	
	insurance	10,000	55,000	300,000
	insurance		75,000	375,000
	insurance		92,000	460,000
	insurance	200,000		200,000
BUSINESS/INDUSTRY	retail bus			150,000
COMMUNICATIONS	TV cable	20,000		
FINANCE	credit bur		15,000 (o)	
	und finance	10,000	50,000	
TRANSPORT/TOURISM				
	transport		10,000 (e)	
	tourism	51,000	185,000	
	tourism	102,000	150,000	150,000
	tourism	100,000		
MISC SERVICES	marketing	500,000 (o)		

We will divide our analysis of the transfers of very large volumes of personal data into three sections. The first will deal with the group that is most in evidence in the figures in Table 9-2: insurers. With 11 transferors of large volumes, insurers account for more than half the transferors of large volumes in the private sector. The second section will deal with other private sector transferors of large volumes. The third section will conclude with an examination of public sector respondents. It should be noted that we will not consider the responses as to country of destination for personal data flows, something that will be examined in Part Five.

9.1 *Insurers*

Insurers that transferred large volumes of personal data were mainly large firms: nine of the 11 respondents reporting very large volumes transmitted estimate their number of clients at more than 100,000, while one estimated this number at between 50,000 and 100,000 and another at fewer than 10,000. We therefore have a very high concentration of large insurers here. Two profiles of the transferors of very large volumes of personal data in this subsector appear relatively clearly: life insurers that transfer personal data to the Medical Information Bureau (MIB) in Boston and insurers that are subsidiaries of an American company. We might also imagine that some respondents are both subsidiaries of an American company and transfer personal data to the MIB either directly or through the American head office. This is what one of our respondents wrote.

9.1.1 Subsidiaries

Subsidiaries of foreign companies are easily identifiable, because question 4 allows us to determine whether the respondents who transfer personal data abroad do so within the same multinational or conglomerate. We can accurately determine that six of the 11 respondents apparently transfer personal data to the American head office (the country of destination, as we will see in the next section, is always the United States of America) of the same multinational. Of these six respondents, four also transferred data about their employees for personnel management purposes, the volumes being obviously much lower. The purposes of the transfers about clients varied from one respondent to another. For example, three respondents reported transmitting data for, among other reasons, later unspecified use. Three respondents also reported transmitting data for purposes of determining eligibility for a service, while three respondents reported transmitting data for the production of statistics. These differences may explain variations in the nature of the personal data transferred by respondents.

The responses to question 7, relating to the nature of the data transferred, show that subsidiaries of multinationals transferred considerably more types of data than did the other transferors of very large volumes in the insurance group. Out of five such respondents, all were subsidiaries of foreign insurance companies. If we go back to the typology of the data that we used in Section 8 of this Part, we find that they all apparently rely on identifiers, this fact being their only common denominator. Among the types of data most frequently transferred abroad were socio-economic status (experience, employment, education) and health (medical history, state of health — although none of the respondents transferred data on psychological tests). Two of these respondents transfer data about what we described earlier as physical characteristics: blood group. None of these respondents reported transferring information in the other categories: legal history and the particularly sensitive category of memberships and affiliations. It should be noted that the respondents, when filling in the questionnaires, could not establish a correlation between the type of information and the type of people (employees, clients). This may explain, in part, the difference between the quantity of types of data transferred by this group compared to life insurers transferring data to the MIB.

Question 8 of our survey asked for details as to the methods of transferring personal data so that we could determine whether all data about all individuals were transferred abroad or only some items taken from individual files or sets of individual files. We were surprised to find that four of these six respondents reported transferring only certain information items from an individual file. Two also reported transferring a series of information items taken from a series of individual files, something that may seem more plausible. We could not understand how such high volumes of personal data could be transferred for one individual at a time. This phenomenon might perhaps be explained by the fact that each insurance policy renewal is the subject of a transfer abroad of personal data using a direct link with the insurance company's head office computer. This hypothesis is particularly plausible because five of these six respondents use some form of telecommunications to data transfer, i.e., transfer of personal data by their own services.

Finally, in question 10 relating to protection and guarantees, two of these six respondents reported that the data subjects were always informed of disclosures to foreign transferees. Two others reported that subjects were informed in certain cases and the other two reported that the people concerned were never informed about such transfers. What might seem even more surprising is that, while a person may not be aware that data about him or her are being transferred, he or she can obtain access abroad to the data transferred and correct it, if necessary. This incongruity may, however, be explained by the fact that, when a person asks an insurer to make corrections in his or her records (for example, a change of address), the practice of transferring any change involving certain items in each client's file results in an automatic correction to the index at the head office.

We will now look at the differences between subsidiaries of multinationals and life insurers that transfer personal data to the MIB.

9.1.2 Life insurers and the MIB

We were able to identify life insurers that transfer personal data to the MIB using question 6 relating to the countries or states to which personal data are transferred. As we noted earlier, the MIB is located in Boston, Mass. For the three insurers that transferred large volumes of personal data and reported transferring this data to the state of Massachusetts, there was a presumption (which was, of course, not irrefutable) that the transferee was, in fact, the MIB. The figures for question 4 (which was designed specifically to identify the transferee) were unfortunately not of great assistance to us in that some respondents saw the MIB as a distinct firm trading in information, while others described it simply as a distinct private firm, not seeing the commercial nature of its activities. The very large similarity between the questionnaire results for these three respondents tends to confirm our initial presumption.

First, the answers to question 5 (relating to the purpose of transferring the personal data) were exactly the same: the data were transferred to determine eligibility for a service (in this case, life insurance). Next, the results for question 7 (relating to the nature of the personal data transferred) were similar but not identical. In addition to family and given names and date and place of birth, data relating to health were most common (medical history, state of health, results of psychological tests and health insurance number). We also found information relating to employment and financial history, with one respondent reporting that it transferred data on criminal or penal record. In question 8, the three respondents reported disclosing a few information items taken from an individual's file, which is not surprising because the same three respondents reported transferring these data by telecommunications. With respect to protection and guarantees, the forms signed by life insurers' clients authorize investigation and disclosure of information about them, something that explains why they all responded that the data subjects are always informed of these disclosures. One respondent also sent us the agreement between insurance companies and the MIB, which contains provisions relating to the confidentiality of personal data.

Finally, we should note that of the two other insurers that we could not classify in either of the two categories, one seems to have a profile compatible with that of a life insurer that transfers personal data to the MIB. It transferred these data to a single American state, but it did not see fit to identify the state. We cannot, therefore, say with certainty that this was indeed a link with the MIB. We found perplexing the fact that the other respondent reported that it transferred personal data to more than 31 American states.

9.2 *Other private sector exporters*

The fact that this is a residual category of private sector transferors of very large volumes of personal data obviously makes generalizations problematic. For example, we may observe that there are both small and very large firms in this category. In fact, of the 10 firms that fall into this category, five of them reported more than 100,000 clients while four others reported fewer than 10,000. As well, while three of the 10 transferors of large volumes reported more than 1,000 employees, five others reported fewer than 100. It should be noted that the firms with low numbers of employees were not necessarily the firms with the fewest clients. For example, one transportation company reported more than 1,000 employees and fewer than 10,000 clients (which is hardly surprising) and a company operating in the tourism sector estimated its number of clients as over 100,000 while it reported fewer than 100 employees.

What is probably most distinctive about these transferors of large volumes of personal data is the categories of persons who were the subjects of the data disclosed. For example, one of the 10 respondents reported transferring data about its employees, two others reported transferring data about neither their employees nor their clients, and the other seven disclosed data about their clients.

9.2.1 *Transfer of very large volumes of data about employees*

The profile of the transportation firm that transferred personal data about its employees is clearly different from the other respondents. Of course, these data were transferred to part of the same multinational. It is not surprising that the purpose of disclosure was primarily personnel management, given that the firm transferred data about the same individual 12 times during the year. However, other purposes such as the production of statistics, storage of data for later unspecified use and, more intriguingly, determination of eligibility for a service were also mentioned. However, it is more probable that the issue here was determination of eligibility for a benefit (a benefit to an employee under a collective agreement, for example) rather than for a service.

Of all the private sector respondents, apart from insurers, who transferred large volumes of personal data, this firm transferred the largest number of types of data about the individuals concerned. Clearly, the various identifiers accounted for a large proportion of these types of data; however, we also found information on people's socio-economic status (particularly in connection with employment history), health (including results of psychological tests), physical characteristics (photograph) and memberships and affiliations (union membership).

With respect to the methods used for these transfers, this respondent reported transferring a series of information items taken from a series of individual files as well as all information held on an individual. When we couple this response with the results of the following question on forms of transfer, we may hypothesize that the series of information items taken from a series of individual files was transferred on magnetic media, while the complete file of an individual may have been transferred in hard copy form or orally (by telephone).

The employees affected by these transfers were never informed of this practice, although they could make corrections if necessary. The respondent reported obtaining guarantees with respect to the use of the data, the relevance of the data to the user, the confidentiality of the data, the security of the data and the time the data would be held in certain cases only. This response is obscure in that there is only one transferee, unless distinctions are drawn between various categories of employees who might have different degrees of protection. This hypothesis is, however, unlikely.

9.2.2 *Transfer of very large volumes of data about individuals who are neither employees nor clients*

The two firms that transferred personal data relating to neither their clients nor their employees were involved in trading in information. They were small firms, both in terms of number of clients (fewer than 10,000) and number of employees (fewer than 100). However, they transferred very large volumes of personal data either to determine an individual's eligibility for a service (direct marketing service) or for customer service purposes (credit bureau). In the case of the credit bureau, the transferee of the data was a firm in the same group, while the direct marketing firm transferred its data to one or more distinct private firms.

The number of information items on each individual transferred abroad was particularly small. The credit bureau reported sending only individuals' credit ratings abroad, while the direct marketing firm sent only family and given names, address and telephone number, language of communication and sex.

These responses leave us somewhat perplexed. It is hard to see how a direct marketing firm can help anyone determine eligibility for a service solely on the basis of language of communication or sex, unless these are in fact distinct lists prepared on the basis of certain characteristics (which our questionnaire could not have discovered because it concentrated on the nature of the data itself). Moreover, this respondent reported transferring all data that it held on all individuals.

Still more surprising is the response of the credit bureau. While it reported transferring nothing but the credit rating abroad, it told us in the same breath that it transferred all data on all individuals. In order for a credit bureau to give an individual a credit rating, the amount of information it would have to hold can be considered phenomenal.

With respect to the form of disclosure, paper-based media were not used. The direct marketing firm transferred its data on magnetic media. The credit bureau transferred its data either by telephone or by telecommunications, the data being transferred by a voluntary action of the credit bureau or by direct access from abroad to the data in its data banks in Canada.

Finally, with respect to guarantees and protection, the two respondents were at the two extremes of the spectrum we outlined. First, the direct marketing firm reported that the people affected by the data transfers were never informed of these transfers and that they could neither obtain access to, nor correct, the data. It is not surprising that the transferee offers no guarantee as to the use or confidentiality of the data transferred because it apparently intends to use the data to solicit sales. On the other hand, the credit bureau reported that the individual who was the subject of the data transfer was always informed of the transfer (the respondent even notes that the individual provided consent), that he or she may have access and make corrections to it and, finally, that the transferees all provided guarantees as to the use, confidentiality and security of the data and the length of time the data would be held.

9.2.3 *Transmission of very large volumes of data about clients*

Here again, we find an odd situation about which it is difficult to make generalizations. Even in the tourism subsector, which accounts for three of the seven responses that we have not yet analyzed in this section, it is impossible to find common traits. Nonetheless, we will note certain factors that might constitute a profile that would be applicable to some of our respondents.

The first similarities are found in the area of purposes. Five of the seven respondents reported transferring personal data solely for client service purposes, a broad and not very meaningful category. Among these five respondents, four reported transferring this information to another distinct private firm or individual, while the fifth did not respond to this question.

In responding to question 7 (dealing with the nature of the data transferred abroad) we first note that these respondents disclosed relatively few data concerning one individual since only one of these five respondents reported transmitting more than five types of data to transferees abroad. In addition to name, address, telephone number and an identification number, that respondent transfers data relating to sex, language of communication, marital status and credit rating. These are all the data that it held on a single individual. It disclosed by direct telecommunications access from abroad. For the other respondents, the number of information items transferred about a single individual was more restricted. For example, in addition to an individual's name and address, a union disclosed date of birth, social insurance number and union membership. These were only a few items drawn from an individual's file. In the case of a TV cable company that used the services of an American firm to bill its clients, only the name, address, amount of the bill and another identification number were transferred abroad. Here again, only a few information items from an individual's file were transferred. For one firm operating in the tourism field (group tours), only the name, sex and telephone number were disclosed. This represented all the data held on an individual. For an investment company, only the name, address, social insurance number and another identification number were transferred abroad, these being only a few of the types of data held on a client.

With respect to the form of disclosure, paper seems to have retained its popularity, three of the five respondents using paper media. However, three respondents reported also using media connected with computers (magnetic media and telecommunications). A majority (three out of five) of the respondents also reported that the individuals concerned were always informed of the disclosure of data concerning them. An investment company even reported that data concerning a client did not cross Canadian borders unless the client had expressly so requested. The TV cable company also reported that no information about its clients was held abroad because once the billings were done they were sent back to Canada. This respondent estimated the annual number of data transfers at one per person. However, unless billing was done only once a year, it is hard to understand this firm's response. How can we imagine monthly or bi-monthly billing being done and personal data not being held abroad? This contradiction is perhaps only superficial. Only a field study with interviews would give us a true picture of the situation.

With respect to the two other respondents whom we have not yet considered, suffice it to note the following factors. Although the first exporter operated in the tourism subsector, its profile was strangely similar to the description we gave of the insurance companies that transferred their personal data to another part of the same multinational firm. The second reported transferring the names and addresses of all its clients, without their knowledge, to a distinct firm trading in information for direct marketing campaign purposes.

9.3 *Public sector exporters*

We have already noted that only a very small proportion of respondents in the public sector transferred very large volumes of personal data (five of the 211 exporters in this sector). On analyzing the responses of the four respondents in the government group, we found a very clear profile. The fifth respondent was in the health services subsector and must be considered as an isolated case.

The organizations in the government group were large departments. Only one of them estimated its staff at fewer than 1,000 employees (between 500 and 1,000 employees). Two of these departments were under federal jurisdiction, the two others under provincial jurisdiction. Certain indicators lead us to believe that these are departments of one of the two large central Canadian provinces.

In the case of three of the four respondents, the data transferred abroad concerned not only people under their administration but also employees and persons who were reported to be neither employees nor clients. Data transfers relating to employees were very small, none exceeding the 10 types of information figure. However, the fact that one department reported transferring data on people who were neither clients nor employees did surprise us. Only this last category showed very large volumes of personal data transferred abroad. For example, during the previous year the number of clients affected by disclosures of personal data to transferees abroad was 40, the number of employees was five and the number of "other" persons was 5,453. Fortunately, however, the person who completed the questionnaire sent us an explanatory letter. Suffice it to note, in order to preserve the confidentiality of our respondent, that the personal data held by this department were transmitted to other government organizations which, according to our respondent's explanatory letter, "may, if they deem it appropriate, transmit this data to other countries". We assume that our respondent was telling us that data were transferred to other organizations knowing that these data were destined to be transferred abroad and that this decision was not the respondent's to make.

The transferees of these personal data were clearly distinct public organizations for these four respondents. What is surprising, however, is that two respondents also reported transferring personal data to a distinct private firm or individual. The only purpose of such transfers stated by the four respondents was the application of a law, regulation or public program. Three respondents transferred personal data in order to determine a person's eligibility for a service while two respondents, who also reported transferring data about their employees, disclosed data for personnel management purposes. One respondent reported that personal data were transferred to apply an international agreement. The only surprise comes from one respondent who reported transferring data for storage abroad for an undetermined later use.

The types of data transferred abroad by these public sector organizations may be fairly numerous. For example, the respondent who transferred the fewest types of data disclosed six types while the others disclosed 18, 24 and 32 types, respectively, and so must be considered differently from private firms that only very rarely transferred more than about 10 types of data.

The organizations and departments that transferred the most diverse data were, in fact, also the ones that transferred data about more than one category of people. Thus, we should not be surprised if an employer transferred data about union membership or other association membership (such as a professional body) for personnel management purposes, particularly when some of its employees were working abroad. On the other hand, this sort of practice could pose a problem if the data subjects were clients. For one of our respondents apparently involved in the administration of criminal justice, the data transferred abroad concerned such sensitive information as fingerprints, photographs, criminal records and association memberships. This respondent sometimes transferred all data held on an individual and sometimes only a few items from an individual's file. Two other respondents reported they may transfer many identifiers. Several information items relating to socio-economic status (financial history, current financial situation, education) and health (medical history, state of health, results of psychological tests) may also be disclosed.

What is surprising, however, is that, in respect of memberships and affiliations, not only data relating to a union or other associations were reported transferred but also data on religious affiliation. What can this information be used for?

These transfers may comprise a series of information items taken from a series of individual files unless they relate to a single individual about whom only a few items are disclosed.

The fourth respondent reported disclosing only six types of data to foreign transferees: names and addresses of individuals together with date of birth, social insurance number, employment information and medical history.

Public departments and organizations also seem to use paper (they all use it) but this traditional form is supplemented by transfers using magnetic tapes (one respondent) and telecommunications (two).

With respect to guarantees and protection, three of the four respondents reported that all persons concerned by such data transfers were always informed that they occur. These persons may generally have access to data thus transferred and may have corrections made if necessary. These same respondents, however, reported that they did not always obtain guarantees from transferees in respect of the use, security and confidentiality of data and the time the data transferred would be held.

This completes the description of the profile of respondents in the government group who reported disclosing very large volumes of personal data. There remains an exceptional case, which we shall deal with briefly here. This is a pediatric hospital that reported transferring personal data to a firm in the same group or conglomerate for purposes of producing statistics. It is not clear that these transfers in fact permitted identification of the individuals concerned. In response to question 7, dealing with the nature of the personal data transferred abroad, no name, address, telephone number, or even an identification number, was transferred abroad. Date of birth, sex, national or ethnic origin, blood group, medical history and health were the only data taken from an individual's file for transfer. This response was, however, not consistent with the response to question 10 dealing with protection and guarantees, where the respondent reported that the people concerned may have access abroad to the data transferred. How could they do so if these data are devoid of nominal information? Moreover, what purpose would be served by the guarantees that our respondent stated that it received from the data transferee in respect of the confidentiality of the data?

9.4 *Summary and conclusions*

Our analysis of the results of all the questionnaires of the 26 respondents who reported transferring very large volumes of personal data highlights several very interesting facts. First, it should be noted that 13% of the private sector respondents who reported transferring personal data abroad disclosed very large volumes of personal data. The proportion for the public sector was barely 2%. This means that more personal data are disclosed by the private sector than by the public sector. However, it should be noted that our analysis is based only on the responses that provided us with a specific estimate of the volumes of data transferred and, so, it is essentially illustrative. It may well be that, among the exporters that responded to the question without estimating volumes, there was a certain proportion that in fact transfers very large volumes. It is, therefore, difficult to extrapolate for all respondents from the 26 analyzed here. However, we might think that very large volumes are much more common than our respondents reported. The lack of precision also indicates decentralization of operations or an inability to estimate that is particularly surprising in that very large volumes are usually transferred using computers, a technique that allows for very precise controls in carrying out these operations.

In the private sector, the insurance group transferred by far the most personal data of any of our respondents. We found that there were two profiles in this group. The first describes the practices of life insurers that transfer mainly personal data about an individual's health to the Medical Information Bureau. The second refers to insurers that transfer large amounts of data to another part of the same multinational, undoubtedly the head offices of these firms. Apart from insurers, the remainder were an assortment of private sector respondents who reported transfers of large volumes of personal data. In order to distinguish them, we decided to separate them on the basis of the people about whom the data were transferred. We prepared a profile of personal data exporters that disclose data about their employees, a feature of the subsidiaries of multinationals. A second profile relates to respondents who report transferring personal data about neither employees nor clients. We found that these were small firms in terms of numbers of both employees and clients and were, in fact, firms trading in information. The last profile in this category, respondents who transfer data about their clients, is much more diverse. However, we may observe that a majority of these respondents relied on foreign firms to process certain data they held about their clients.

Finally, the few public sector respondents who transfer very large volumes of personal data abroad were mainly departments and other government organizations. These government group respondents reported that they transferred data not only about the people under their administration but also about employees (very few cases) and individuals who were neither employees nor clients. Here we should add that these organizations may have transferred a large number of items of personal data, ranging from simple identifiers to data that are as sensitive as religious affiliation.

PART FIVE

COUNTRIES OF DESTINATION AND LEGAL PROTECTION

We wanted to pay particular attention to the results of our survey identifying the countries of destination of transborder personal data flows from Canada, and so we decided to devote a fifth part to this subject. In this part we have two objectives. The first is to set out the results of our study of the countries of destination of transborder flows. The second is to assess the legal protection accorded to personal data transmitted outside Canada, at least in those countries most frequently cited by respondents.

For these purposes, we wanted to tie the results of our survey as closely as possible to the results of our study of the legislation. We will, therefore, consider the question of the legal protection given to personal data leaving Canada immediately after identifying the countries of destination for these data. In this process, we will retain the general outline we have used so far: describing the results from the most general to the most specific. After considering (1) the overall situation and the groups of countries that provide protection in both the public and private sectors, we will examine, in order, the transferees and the protection offered (2) in the public sector in general and (3) in the private sector in general and close with (4) an examination of specific situations, sector by sector.

With respect to the survey, it should be noted that the questionnaire enabled us to determine the destination of transborder personal data flows with relative precision. To identify the countries in question, we provided a number of choices (the United States, Great Britain, France, Japan and the Federal Republic of Germany) and also suggested other countries on the various continents (other Western or Eastern European countries, other Asian, African or South Pacific countries). In these cases, we asked that respondents list the two or three most important countries of destination to which personal data were reported to be transferred. Similarly, for federal countries, such as the United States and the Federal Republic of Germany, we asked them to indicate the various provincial jurisdictions (state and country) where data were sent. In the specific case of the United States, we asked that they check off whether flows involved only one state and, if so, what state or several states (two to five states, six to 10 states, 11 to 30 states, and 31 to 50 states), in which case we also asked them to name the three most important states. Respondents also had the choice of reporting whether they sent data to more than 20 countries or more than 50 countries.

It should be noted that some respondents did not identify particular countries, noting in the margin that anything was possible depending on the requests they received. This situation arose essentially in the health services and education sectors. In that case, we entered "no response" for this question because such a response did not give us precisely the information requested and would have distorted the situation if we had entered a response on behalf of the respondent.

We would note that one respondent from a medical centre also observed that anything was possible but, nonetheless, reported more than three countries per region. We could not include them all, which was unfortunate for the Dominican Republic which was ranked fourth only by this respondent! As well, one federal organization noted that, in its field of activity, Canada had signed agreements and treaties with several countries: Austria, Bolivia, Cyprus, Denmark, Finland, France, Greece, Mexico, Morocco, Peru, Spain, Sweden, United Kingdom, United States of America (28 states). However, that organization did not tell us whether, in fact, it engages in data flows to these countries, and so we had to enter "no response" to this question.

To determine the countries for which we would have to study the legislation, we used two tests: the number of respondents who report exporting data to a single country (occurrences) and the destinations of the highest volumes of flows. We will, therefore, examine only the jurisdictions to which significant flows took place in terms of occurrences and volume.

1 Overall situation

In this first section, we will analyze the responses to question 6 of our questionnaire to determine the most important destinations for personal data transfers for our respondents as a whole. We will then determine the countries to which significant flows of personal data are transmitted.

This procedure is inadequate in that several respondents transfer small volumes of personal data, which could eclipse some respondents who transfer very large volumes. We will therefore compare the results of question 6 with the results of subquestions 3(c), (d) and (e), dealing with the volume of personal data transferred abroad. Secondly, we will attempt to determine a typology for the legal coverage provided by the personal data protection offered by the various countries. Finally, we will consider the broad types of legal protection of personal data adopted by the various groups of countries on the basis of the typology we establish.

1.1 Overall results of the survey

The first two conclusions to be drawn from our survey may appear contradictory. First, there are very few countries in the world that do not receive personal data transmitted from Canada — from Australia to Zimbabwe, with Nepal and Macao, Botswana and Burkina Faso, Vanuatu and Fiji, the Soviet Union and Yugoslavia, and Chile and Nicaragua along the way. In total, more than 100 countries or territories (such as Hong Kong) were identified by our respondents as destinations for their transborder flows. And only 10 American states (Arkansas, Delaware, Idaho, Iowa, Kansas, Kentucky, Louisiana, Nebraska, New Mexico, Rhode Island) were not mentioned by any respondent as a potential destination. It might also be noted that 26 respondents reported transmitting personal data to more than 20 countries, while 17 respondents reported sending data to more than 50 countries.

Our first observation is that personal data on Canadians and foreigners living in Canada circulate in a majority of the countries of the world. Although the industrialized countries, and particularly the OECD countries, are the most important destinations for personal data transfers, several developing countries are also included. For example, the list of the 25 main destinations for personal data transfers by Canadian firms and organizations listed in Table 1-1 includes 12 industrialized countries that are members of the OECD, 12 developing countries (some of which could also be termed newly industrialized countries although we will not employ this distinction) and one territory, Hong Kong, which is still connected with the United Kingdom for a few more years.

Table 1-1
The 25 main countries of destination

1 - United States of America
2 - United Kingdom
3 - France
4 - Federal Republic of Germany
5 - Japan
6 - Australia
7 - Hong Kong
8 - Italy
9 - New Zealand
10 - Switzerland
11 - Mexico
12 - Jamaica
13 - Singapore
14 - Portugal
15 - Brazil
16 - India
17 - Belgium
18 - People's Republic of China
19 - Greece
20 - Malaysia
21 - Thailand
22 - Barbados
23 - Colombia
24 - Pakistan
25 - Philippines

We cannot rely on these findings, however, because they might mask the real situation. While the number of destinations reported is impressive, and as many developing countries as OECD countries appear, it must not be forgotten that the primary destination for transborder personal data flows is the United States of America. More than 17% of respondents report transmitting personal data to the United States.

This means that more than 81% of those respondents who report transmitting such data do so to our neighbours to the south.

Table 1-2 indicates the numbers of occurrences for certain countries and by continent, as well as the percentage of such occurrences in relation to the total number of respondents (1,763) and in relation to the respondents who reported personal data transfers (373).

Table 1-2
Transfers by country or continent

Country/continent	Occurrences	Occurrences /N respondents (%)	Occurrences /N exporters (%)
United States of America	303	17.19	81.23
Great Britain	126	7.15	33.78
France	95	5.39	25.47
Western Europe	69	3.91	18.50
Federal Republic of Germany	65	3.69	17.43
Asia	61	3.46	16.35
America	61	3.46	16.35
Japan	56	3.18	15.01
South Pacific	50	2.84	13.40
Africa	47	2.67	12.60
Eastern Europe	25	1.42	6.70

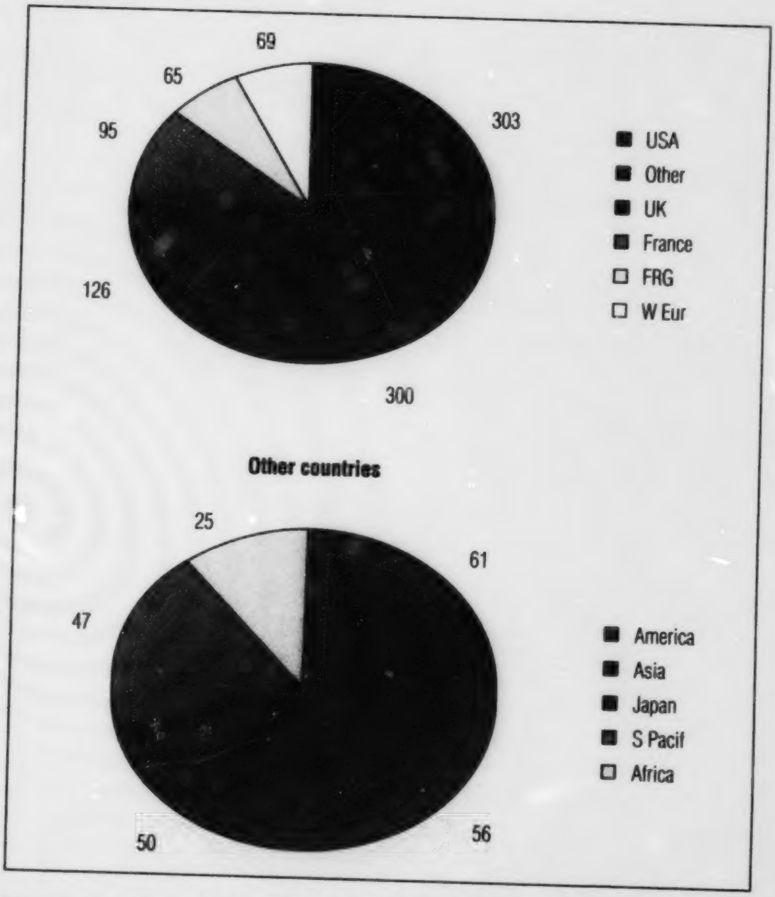
It must be noted that very few countries receive a significant amount of personal data from Canada. If our criterion for measuring significance was the fact that at least 1% of respondents sent personal data, only eight countries could be considered in this category, as Table 1-3 shows.

Table 1-3
Significant destinations in terms of occurrences per country

Country	Occurrences	Occurrences /N transferors (%)
United States of America	303	17.19
Great Britain	126	7.15
France	95	5.39
Federal Republic of Germany	65	3.69
Japan	56	3.18
Australia	26	1.47
Hong Kong	21	1.19
Italy	20	1.13

This table is not extremely surprising overall. The United States, our primary trading partner, is at the head of the pack, as would of course have been expected. It is followed by the European countries: the United Kingdom, France, the Federal Republic of Germany and Italy, which have supplied the largest share of the people who make up the Canadian population and with which our economic and cultural ties have survived the test of time. The presence of Japan, Australia and Hong Kong in fifth, sixth and seventh place clearly shows the burgeoning of economic activities in the Pacific region in the last few years.

Graphic 1-1
Transfers by country or continent



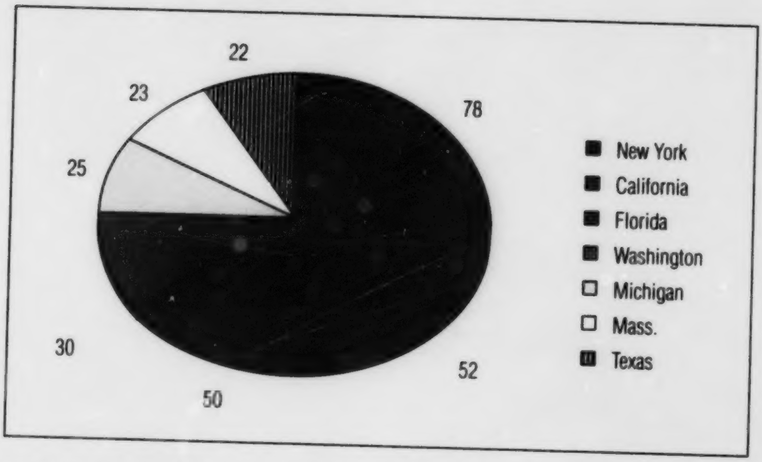
If we now include the political subdivisions of the United States to which more than 1% of respondents reported sending personal data about Canadians, the picture changes radically. As Table 1-4 demonstrates, for eight different countries to which more than 1% of respondents reported transmitting personal data, there were seven American states to which at least as many respondents reported sending such data (and again we must note the presence of Hong Kong, which could be termed a political subdivision of the United Kingdom). These figures provide us with a better indication of the predominance of the United States as a destination for transborder personal data transfers. In this table, the asterisk (*) indicates an American state.

Table 1-4
Significant destinations in terms of occurrences (including American states)

Country/state	Occurrences	Occurrences /N of respondents (%)
United States of America	303	17.19
Great Britain	126	7.15
France	95	5.39
*New York	78	4.42
Federal Republic of Germany	65	3.69
Japan	56	3.18
*California	52	2.95
*Florida	50	2.84
*Washington	30	1.70
Australia	26	1.47
*Michigan	25	1.42
*Massachusetts	23	1.25
*Texas	22	1.19
Hong Kong	21	1.19
Italy	20	1.13

It is not surprising to find listed the important states (such as Washington, Michigan, Massachusetts and New York), that border or almost border on Canada, the large southern states such as California or Texas, or a state like Florida, which is the destination for many Canadians each year. In Table 1-4, only the number of occurrences for the various destinations is counted. However, because our questionnaire asked for two or three destinations for each continent, we have weighted the results by assigning three points for a first choice, two for a second choice and one for a third choice. This exercise did not reveal any significant differences from the results already obtained.

Graphic 1-2
American states of destination



We also compared the results for question 6 concerning destination with the results for subquestions 3(c), (d) and (e) dealing with volume. Noting that some firms export very large volumes of personal data, we concluded that we would have to examine the legal systems applicable to these data. A single occurrence in which data about more than 10,000 people are transferred abroad is equal to dozens of occurrences in which data about only a few people are transferred abroad. In Table 1-5 we set out the cases in which very large volumes are sent to single destinations.

Table 1-5
Single destinations for very large volumes

State	Subsector	1 year (10,000+)	5 years (10,000+)	total (100,000+)
Massachusetts	insurance	75,000	375,000	
	insurance		10,000	
	insurance	92,000	460,000	
Florida	insurance		20,000	
	tourism	51,000	185,000	
	hospital	15,000		
Washington	insurance	200,000		200,000
	union		20,000	
California	ret/whol bus			150,000
	communications	20,000		
Pennsylvania	insurance			12,000
Illinois	insurance	40,000		
New York	insurance	150,000	600,000	150,000
Missouri	tourism	102,000	150,000	150,000
Connecticut	transportation		10,000 (e)	

In Table 1-5, (e) denotes the number of employees; in all other cases figures refer to clients. We see from this table that the only destinations for very large volumes were American states, and that all, with one exception, were in the private sector. We will return to the figures in this table when we do our sectoral analyses.

We will therefore in this section consider the legislation that is applicable in the following countries and states: the United States, California, Connecticut, Florida, Illinois, Massachusetts, Michigan, Missouri, New York, Pennsylvania, Texas, Washington, the United Kingdom, France, the Federal Republic of Germany, Japan, Australia and Hong Kong.

As well, when we analyze the figures for the various groups of subsectors, we will discover that other states may be more significant destinations in a given industry.

As we have seen when we dealt with transferees in point 6 of the preceding part, few respondents actually identified their transferees precisely. For those who did, we found that 80% of private sector respondents reported engaging in intra-corporate flows (i.e., within the same multinational or conglomerate). In the public sector, 82% of respondents reported sending their data to distinct foreign public organizations. It should be noted, however, that 40% of these public sector respondents also sent flows to private sector organizations. However, while there is nothing in these figures from which we could identify the transferees, we can hypothesize that some transferees such as hospitals or colleges and universities, which are private abroad, may be public in Canada. In the private sector, only 14% of respondents reported sending flows to foreign public organizations but, there again, we could not identify them.

We will therefore consider, for the purposes of our study of legal protection, that when a respondent transmits personal data abroad it does so to a transferee that operates in the same subsector of activity. For example, we will assume that an educational institution that transfers personal data sends the data to another educational institution, and will accordingly examine the legal provisions in the country of destination that would specifically govern the question of school records, for example. While we may assume that most of the time the transferee operates in the same subsector of activity, we might well find transfers to firms in other subsectors (e.g. a university that transfers personal data about a former employee to a firm that specializes in personnel recruitment). However, given that this is an uncommon situation on which our study does not provide details in any event, we will take for granted that the exporter and the transferee are in the same sector.

1.2 *Typology of countries of destination*

We now intend to examine the legislation protecting personal data in the countries and jurisdictions to which data flow from Canada, in light of the results of the survey. We do not wish to restate the work already presented by GRID[1], which sets out a detailed presentation of the legislation of various countries, using a number of American states as examples and for purposes of illustration. We will assume that the results of this work are known.

We propose to set out the legal protection enjoyed in other countries for data originating in Canada, according to the following outline. First, we will set out the general legislation that covers both the public and private sectors and governs the protection of personal data in each of the types of countries that we have isolated. For each of the jurisdictions that we have identified as significant, based on the results of our study, we will then examine personal data protection in the public sector, followed by the private sector. Obviously, each section will not restate the general results, which will be set out first, but rather will examine only the specific and peculiar aspects of the public or private sectors, taking for granted the considerations and general protection initially examined.

We will end this description of legal protection with an examination of the protection that is specific to each of the sectors we have identified in our study as transferees of flows. Of course, when general legislation or legislation covering the public or private sector exists in a jurisdiction, we did not consider it necessary to research whether there are specific legislative provisions in a particular sector. For example, if our study indicates significant flows to France in the education sector, we did not consider it necessary to research whether there were specific legislative provisions in education because in France there is general privacy protection legislation. Accordingly, when there is general legislation, we have not found it necessary to research specific or sectoral provisions; however, this does not mean that such provisions do not exist.[2]

---

[1] LAPERRIÈRE, René and PÉLADEAU, Pierrôt, *Le droit sur la protection des renseignements personnels: Étude sur les bases privées de données à caractère personnel en droit canadien, comparé et international*. Montreal, 1986, SOQUIJ, 456 p.

We conducted a systematic examination of the legal data in our possession on the state of the legislation in various countries of destination for personal data flows. In addition to the publications and records of GRID, including a data bank on legislation in this field, we also used the publications of the Privacy Journal[3] and the CCH Guide to Computer Law with regular updates, as well as the various legislative repertories on law and computers and on the concept of privacy.

As we indicated in Part One, we wrote to the privacy commissioners in those countries that have privacy legislation to find out whether their legislation covered foreigners whose data might be stored on their national territory. This is a question of private international law that is important to an understanding of the degree of protection enjoyed by personal data about Canadian citizens. In this respect, a simple reading of foreign legislation does not tell us whether the substance of the legislation covers personal data concerning non-nationals. We had to seek information from the commissioners. The rate of responses received is indicated in Part One. In examining these responses, we find that the European countries protect personal data about foreigners: data about both nationals and foreigners is treated in an identical manner. Thus, each time it appears pertinent, we will indicate whether the national legislation also protects data concerning foreigners. For the other countries, we will have to keep this question in mind each time.

This review confirmed, first, that few countries overall have legislation to protect personal data specifically. This concern is primarily a European one, several of the European countries having been the first to adopt privacy protection legislation in the 1970s.

---

[2] For example, in banking, new specific legislation in France relates to the creation of an index by the Banque de France on incidents of payment under the 1984 banking law. This law, No 89-1010 of December 31, 1989, respecting the prevention and resolution of difficulties relating to excessive indebtedness on the part of individuals and families, permits a banker not to grant credit to an individual who has been recorded in this index as having too much debt; the procedure provides for no remedy for the client and also permits no written disclosure of the record. However, because this is a sectoral exception to broader general legislation, we did not consider it necessary to refer to it.

[3] Robert Ellis SMITH, *Compilation of State and Federal Privacy Laws*. 1988, Washington, Privacy Journal, 102p.

The European statutes are general in nature; i.e., they cover indexes maintained both in the public sector and in the private sector. Moreover, generally this type of legislation has no provisions covering certain sectors of activity specifically, such as credit agencies or banks, for example. Thus, all sectors, whether they fall within the ambit of government or private enterprise, are in theory subject to the same body of fundamental rules with respect to the management of personal data. There is, however, a trend in the more recent legislation to incorporate particular rules in their substantive provisions aimed at specific sectors of activity. These statutes are often referred to as the second generation.

Nonetheless, this sectoral approach does not operate to deprive these statutes of their general character. These specific rules merely add to the general rules of application. In other words, the specific rules supplement the protection offered so as to ensure greater compliance with the general objective of this type of legislation. Moreover, as the OECD emphasizes in a recent report, these two approaches are not contradictory[4] and may even be complementary. In order to put general principles into practice, it is sometimes necessary to enact specific provisions that are better able to take into account the contingencies and peculiarities of certain sectors.

Other countries, which as a whole have adopted a different legal approach, place greater emphasis on privacy. It is not the object or nature of the information that is at issue, but rather the subject himself or herself, the individual who is both beneficiary and defender of an individual right, such as the right to privacy or the right to noninterference in his or her personal affairs. This different perspective demands different legal tools. In this system, the individual is seen as having primary responsibility for defending his or her privacy, legislation being used only to alleviate excessive inequalities. On the other hand, legislative intervention is piecemeal or case by case, counteracting potential vehicles and sources of privacy violation one by one.

Thus, when it is the government that presents a threat to privacy, restrictions, constraints and procedures in the field of activity in question will be imposed on it. When the threat is posed by private organizations and individuals do not have the ability to defend themselves against it, specific legislation may be enacted to reestablish a degree of equilibrium. In these countries there is legislation protecting personal data but it is piecemeal and specific. It will be noted that, in this group of countries, the legislation tends primarily to restrict governmental or public intrusions into privacy and concentrates mainly on regulating the public sector.

---

[4] OECD, *Situation actuelle et tendances de la protection de la vie privée dans la zone de l'OCDÉ*. Paris, OECD, DSTI/ICCP/88.5, p 18.

Finally, in a majority of countries, protection of nominative data has not been given the priority for it to be necessary to enact specific legislation. In these countries, and it is mainly these which responded to our requests for information, we therefore found constitutional or general legal provisions covering the concept of the protection of privacy or of personal data in principle. Thus, a typology consisting of three categories emerges:

1. Countries with broad and general personal data protection legislation covering both public and private sectors. These are found essentially in the Western European countries.[5]
2. Countries that do not have general legislation but rather a set of specific personal data and privacy protection laws covering primarily the public sector. These are essentially the United States of America, Canada, Australia and Japan.
3. Countries that have no general personal data protection legislation, although certain specific provisions may cover public or private activities, or both, in certain sectors.

We will examine the legislation by grouping countries according to the typology set out above: in point 1.3, the European countries; in point 1.4, the United States of America, Australia and Japan; and in point 1.5, the other countries. We will first examine the general personal data protection system in each of these three groups of countries. Then, after examining each case and noting the figures from our survey, in each case to determine the nature of flows from Canada, we will examine the legislative protection enjoyed by personal data that such flows deliver to each of these countries. For this purpose, we will follow an outline moving from the most general to the most specific, from general legislation covering all sectors to legislation covering only the public or private sector, and concluding with sectoral legislation in the public or private domain.

1.3 *The European countries*

1.3.1 *International instruments*

In examining European legislation on personal data protection, our attention is first drawn to the fact that it is general and all-encompassing. These countries have also adopted international instruments for dealing with the protection they have accorded to personal data.

Taking transborder flows as our starting point, we found two principles affirmed: the free flow of information and equivalent protection or equivalent treatment. Based on these principles, national legislation accords "favourable treatment" to the European countries that are bound by the European Convention by placing more controls on flows to other countries where there is a risk that privacy might be violated.

---

[5] Austria, Denmark, Federal Republic of Germany, Finland, France, Great Britain, Grand Duchy of Luxembourg, Isle of Jersey, Isle of Man, Iceland, Ireland, Netherlands, Norway, Sweden.

Two international instruments concerning personal data protection highlight the application of these principles in Europe. On September 23, 1980, the OECD adopted the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and, on January 28, 1981, the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[6]. These show the importance accorded to transborder data flows in the protection of privacy. Rarely has an issue in international public law resulted in such rapid development of an international instrument. In the space of 10 years, two international instruments were adopted. We would note that the Guidelines are simply a recommendation, having no obligatory effect from a legal point of view[7], while the European Convention is a legally compelling instrument.

We will summarize these two international instruments, both of which cover both public and private sectors. They incorporate minimum standards for personal data protection. These principles are fundamental with respect to personal data management: the collection limitation principle, data quality principle, purpose specification principle, use limitation principle, security safeguards principle, openness principle, limited time of storage principle, accountability principle and individual participation principle. These principles cover the entire scope of the protection of nominative data. Countries may always grant broader protection for nominative data under Article 6 of the Guidelines or Article 11 of the European Convention. The principles set out in the Guidelines and the European Convention are, thus, the lowest common denominator with respect to data privacy protection and are designed to breathe a minimum of legislative harmony into the general law of personal data protection. This is the "hard core" to which member countries are invited to subscribe.[8] Thus, these standards facilitate the circulation of personal data because nominative data are treated in the same way, wherever they are located. A country need not, therefore, worry about personal data concerning its nationals that are exported to a state that has subscribed to the Guidelines or the European Convention, because these data enjoy protection equivalent to the protection enjoyed on national territory. This is the concrete application of the notion of the "hard core" or minimum standards.

---

[6] The European Convention came into force on October 1, 1985, following ratification by five member countries of the Council of Europe (Sweden in 1982; France in 1983; Spain and Norway in 1984; and the FRG in 1985), and is therefore positive law.

[7] OECD, *Guidelines on the Protection of Privacy and the Transborder Flows of Personal Data* (Explanatory Memorandum), Paris, 1980, p 22.

[8] [Translation] "Rather than convincing States to become aware of a problem which, in Europe, is no longer ignored, it is an attempt to convince these States of the advisability of harmonizing national legislation, be it only in this minimal way, around a 'hard core' which should be common ...". LAMY, *Droit de l'informatique* (under the direction of Michel VIVANT), Paris, Éd Lamy SA, 1986, p 329 No 728.

We would also note that present or forthcoming accession to the Convention indicates that legislation applies to foreigners whose data are stored on national territory. Article 1 of the Convention states:

The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, *respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection") (emphasis added).*

On this point, we would refer to the following passage from the Explanatory Report, which makes these comments on the scope of this provision:

The guarantees set out in the convention are extended to every individual regardless of nationality or residence. *This provision is in accordance with the general principle of the Council of Europe and its member States with regard to the protection of individual rights. Clauses restricting data protection to a State's own nationals or legally resident aliens would be incompatible with the convention*[9] *(emphasis added).*

Article 14 of the European Convention requires each contracting party to assist any person residing abroad to exercise the rights conferred by its domestic law, giving effect to the principles set out in Article 8 of the Convention (individual participation principle).

The OECD Guidelines do not contain any provision similar to Article 1 of the European Convention. However, given the general spirit of that instrument and, particularly, articles 15 to 18 relating to transborder flows of personal data, we might argue that legislatures should not arbitrarily exclude foreigners from the protection of the law. The principle of the free flow of information at the international level, which provides the structure for the substance of the Guidelines, would demand that foreigners be treated like nationals in terms of exercising data rights; otherwise, it could be argued that a country would be justified in objecting to data being exported from its territory if its nationals could not exercise their rights of access and correction in the importing country. While the importing country might, for example, have a personal data protection law, the effect of the fact that a foreigner could not assert the rights set out in that law would be to violate the principle of equivalence, the conceptual foundation underlying (and justifying) the free flow of information.

---

[9] Council of Europe, *Explanatory report concerning the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Strasbourg, Council of Europe, 1981, p 21, para 26.

It is also useful to refer to Article 19e) of the OECD Guidelines, which provides:

> *...Member countries should in particular endeavour to:*
>
> ...
>
> *e) ensure that there is no unfair discrimination against data subjects.*

This paragraph appears in Part Four of the Guidelines entitled "National Implementation". The explanatory notes are sketchy as to the interpretation of this provision. It is, however, possible to argue that the authors of the Guidelines intended by this provision to recommend that member countries not discriminate against data subjects in the context of exercising their rights of access and correction. It would also be possible to argue that excluding foreigners might constitute unfair discrimination and that a country could not treat one of its nationals differently from a foreigner in respect of exercising data rights, particularly since the *principle of equivalence* is actually the foundation and conceptual basis of these legal protections.

This principle may also be defined as follows: a country shall not object to the transfer of personal data to a third country where that third country confers, by appropriate legislation or a system of self-regulation, personal data protection substantially equivalent to the protection that exists in the exporting country.

A study of European legislation shows that regulation of personal data exports is based on the principle of equivalence set out in Article 17 of the Guidelines and Article 12 of the European Convention.

We may therefore conclude on this point that the application of national legislation to foreigners (national treatment) is the necessary corollary to the principle of the free flow of information.

In closing, we might note that the Council of Europe has adopted a number of recommendations with respect to personal data protection. These recommendations reflect a sectoral approach, as they relate only to certain very specific sectors of activity[10]. We will deal with these directives when we examine the various sectors.

---

[10] A list of these recommendations clearly shows their sectoral nature:
- Recommendation No R(81)1 (on regulations applicable to automated medical data banks) (23 January 1981);
- Recommendation No R(83)10 (on the protection of personal data used for research and statistical purposes) (23 September 1983);
- Recommendation No R(85)20 (on the protection of personal data used for direct marketing purposes) (25 October 1985);
- Recommendation No R(86)1 (on the protection of personal data used for social security purposes) (23 January 1986);
- Recommendation No R(87)15 (on the regulation of the use of personal data in the police sector) (17 September 1987);
- Recommendation No R(89)2 (on the regulation of the use of personal data in employment) (1989).

These non-obligatory recommendations complete the bundle of protections established by the Convention:

[Translation]
While the principles of data protection set out in the Convention for the Protection of Individuals with regard to Automated Processing of Personal Information ... of January 28, 1981 applies generally to the collection, recording, use and so on of personal data in the public and private sectors, it was felt to be necessary to adapt them to the specific requirements of particular sectors.[11]

As is the case with respect to the legislation, we note that sectoral provisions supplement and refine the general, all-encompassing approach. This is particularly the case for Recommendation No R(89)2 on the regulation of the use of personal data in employment (1989) which applies to both the public and private sectors.

Finally, it should be noted that the European legislation applies to branches and subsidiaries of multinationals operating there and that their operations are subject to the legislation. Similarly, foreign firms must comply with that legislation in offering computer services to European firms.

The various international instruments and national legislation further provide two types of specific protection: first, according to the nature of the data collected; and second, according to the purpose for which the data are gathered.

1.3.2 Protection relating to the nature of the data

In Europe, there is protection generally offered by the international instruments based on the specific nature of the data in question. It can be traced to the actual definition of "personal data", which is similar in any legislation we might examine. This is undoubtedly another example of the normative influence exerted by the OECD Guidelines and the European Convention.

By way of example, the expression "personal data" is defined as follows in Article 1b) of the OECD Guidelines:

"personal data" means any information relating to an identified or identifiable individual (data subject).

This expression is also defined in Article 4 of the French Law:

[Translation]
Within the meaning of this Law, any data from which it is possible, in any manner, whether directly or indirectly, to identify the individuals

---

[11] Council of Europe, statement of reasons, Recommendation No R(87)15 (on the regulation of the use of personal data in the police sector), Strasbourg, Council of Europe, 1988, p 13, para 1.

> *to whom they apply, whether such data are processed by an individual or by a corporate body, shall be deemed to be nominative data.*

With respect to another OECD country, we note section 6 of the Australian Act, which also defines the expression "personal information":

> *"Personal information" means information or an opinion (including information or an opinion forming part of a database), whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.*

There is a consistent thread here. It must be possible to identify the individual from the data if the data are to fall within the scope of this definition and receive the resulting protection. This is the basic requirement in the definition of "personal data" and is found in principle in all legislation.

In addition to this common definition, we also note that some legislation provides specific protection depending on the nature of the data: France provides a specific category relating to "sensitive data" and Great Britain makes provision, in certain circumstances, for additional protection to be accorded to certain types of data. The German statute and the Australian and Japanese legislation, incidentally, do not contain any provision respecting sensitive data.

1.3.3 *Protection relating to purposes*

In terms of protection relating to purposes, we might refer to the purpose specification principle set out in the OECD Guidelines and in the European Convention. Basically, paragraph 9 of the Guidelines implies that in all cases, not later than at the time of data collection, it should be possible to identify the purposes for which these data are to be used and that later changes of purpose should likewise be specified. Such purposes may be specified in a number of alternative or complementary ways, notably by public declarations, information to data subjects, legislation, administrative decrees and authorization by supervisory bodies. According to paragraph 10 (use limitation principle), new purposes should not be arbitrary; changes being made should imply compatibility with the original purposes.[12]

The statutes we have examined adopt the essence of these principles in their substantive provisions. This minimum standard, described above, is thus incorporated into national legislation. Of course, this complies with the concept of a "hard core".

---

[12] Explanatory Memorandum, supra, footnote 7, p 30.

1.3.4 *National protection*

Having examined the general legislation in Europe, we can now analyze precisely the protection offered to personal data in each of the European countries to which large volumes of personal data are transferred from Canada: the United Kingdom, France and the Federal Republic of Germany. We have already noted that legislation in the European countries concerning personal data protection covers both public and private sectors.

UNITED KINGDOM

Great Britain enacted personal data protection legislation in 1984. This Act covers only automated indexes, not manual ones (sec 1(2)).[13] The British Act adopts the fundamental principles with respect to personal data management found in the Guidelines and the European Convention. The British Parliament has instituted a system of registration of data banks. The substance of the Act is rather technical. It describes the registration procedure with everything that this involves (length of time, renewal, inspection, refusal, right of appeal, and so on), the rights of the person indexed (method of exercising, right of appeal) and exceptions to the Act. The fundamental principles are found in schedule 1 to the Act.

In terms of transborder personal data flows, Parliament set out the substance of the European Convention in section 12. The Privacy Commissioner may issue a "transfer prohibition notice" to any person who intends to export nominative data if the importing country does not offer protection equivalent to the protection offered by the British Act, thus adopting the principle of equivalence.

Some provisions permit the Secretary of State to grant additional protection to certain types of data, that is, depending on their nature:

The Secretary of State may by order modify or supplement those principles for the purpose of providing additional safeguards in relation to personal data consisting of information as to

(a) the racial origin of the data subject;
(b) his political opinions or religious or other beliefs;
(c) his physical or mental health or his sexual life; or
(d) his criminal convictions;

and references in this Act to the data protection principles include, except where the context otherwise requires, references to any modified or additional principles having effect by virtue of an order under this subsection.

---

[13] Note the conclusions of our study, which found that 89% of respondents transfer personal data in handwritten form, so that the effects of this Act with respect to personal data transferred from Canada are considerably restricted. See supra, Part Four, point 7.2.

We are not in a position to know whether the minister has in fact adopted specific measures concerning these categories of personal data. In any event, it must be understood that this type of provision can only have a positive impact on personal data concerning Canadian citizens because there would then be supplemental protection.

The British Act contains no provision stating whether it applies to foreigners as well. Ratification by Great Britain of the European Convention implies that the English legislation also covers foreigners. In any event, Mr. Aldhouse of the Data Protection Registrar's office confirmed to us in writing that the British Act applies to foreigners in the same manner as to British nationals.[14]

There are no sectoral provisions in the English legislation.[15]

Finally, we would note that Great Britain acceded to the OECD Guidelines on September 23, 1981. It signed the European Convention on May 14, 1981, and ratified it on August 26, 1987. The Convention came into effect on national territory on December 1, 1987.

FRANCE

The French legislation was enacted in 1978. It is general and all-encompassing in that it applies to the public and private sectors and covers both automated and manual indexes.

The French statute provides a system of prior registration governing the establishment of automated processing procedures. The substance of the Law contains the fundamental principles set out in the Guidelines and the European Convention. The French legislature has created a regulatory body: the CNIL — Commission nationale de l'informatique et des libertés (National Commission on Computers and Freedoms).[16]

Article 24 of the French statute provides that prior authorization may be given by the CNIL for the export of nominative data in order to ensure compliance with the principles set out in the Law. This provision relates only to private transactions.[17] Transfers involving the public sector depend on the relevant international agreements. On this point, Prof. Lucas writes:

---

[14] See the text of the letter attached as Appendix 3.

[15] For a more detailed picture of the British legislation, see in particular Jeremy McBRIDE, "Citizen's Privacy and Data Banks: Enforcement of the Standards in the Data Protection Act 1984 (UK)", [1984] 25 Cahiers de droit 533.

[16] For a complete picture of the French legislation, see in particular André LUCAS. *Droit de l'informatique*, Paris, PUF, 1987.

[17] Ibid, p 68.

> *[Translation]*
> *Nominative data transfers effected between public institutions are subject to international agreements. The same is true for international organizations. France has, for example, signed a basic agreement with Interpol, the international organization of criminal police, to which is annexed an exchange of letters providing for the control of Interpol files by an international commission of five members having different nationalities.*[18]

The French Law also contains a provision protecting personal data by category when addressing sensitive data. Article 31 provides that:

> *[Translation]*
> *The entering or storing in computerized memory, without the express agreement of the subject, of nominative data which discloses, directly or indirectly, an individual's racial origin or political, philosophic or religious opinion or union membership, is prohibited.*
>
> *However, churches and groups of a religious, philosophic, political or union nature may maintain a record of their members or correspondents in computerized form. No control may be exercised over them in this respect.*
>
> *For reasons of the public interest, exception may also be made to the above prohibition upon a proposal or opinion to that effect of the commission [CNIL] to the Council of State.*

Thus the French legislature has placed certain types of data into a separate category and given them special status in terms of privacy protection by virtue of their extremely sensitive nature. This sort of a classification complies with Article 6 of the European Convention. That Article prohibits any transactions involving certain categories of data because of their sensitivity (political opinions, religious or other beliefs, health, sexual life, criminal convictions) unless domestic law provides appropriate safeguards. The French legislature has therefore followed the terms of the Convention.

The body of the French Law does not state whether it applies to foreigners. Nonetheless, given our comments in point 1.3.1.1 on Articles 1 and 14 of the European Convention (which essentially provide that the rights set out therein apply to individuals regardless of their nationality or residence), it seems to us to be entirely justified to assert that the French legislation covers nominative data stored in France concerning foreign citizens.

The French Law contains no sectoral provisions.

Finally, we would note that France acceded to the OECD Guidelines on September 23, 1980. It signed the European Convention on January 28, 1981, and ratified it on March 24, 1983. The Convention came into force on October 1, 1985.

---

[18] Ibid, p 69.

FEDERAL REPUBLIC OF GERMANY

The West German legislature enacted a personal data protection statute in 1977. The West German legislation applies to the public and private sectors, and covers both automated and manual indexes. The legislature has adopted the fundamental personal data management principles recognized in the Guidelines and the European Convention.[19]

There are no specific provisions covering transborder data flows in this legislation. However, the exportation of personal data is treated like any other transfer.[20] Accordingly, national rules governing the transfer (disclosure) of personal data also apply to international transfers, the rules on domestic transfers being transposable to the international context. The rule that can be seen in examining the body of the statute relates to the preservation of the (privacy) interests of the persons on whom information is held. By transposing this to a transborder context, we conclude that the principle of equivalence comes into play.[21] The interests of the data subject could not be preserved in the case of an international data transaction unless the importing country offered protection for the nominative data exported that was analogous to the protection enjoyed on German territory.

There is no section specifying whether the German legislation also covers data about foreigners. Mr. Stange, the Privacy Commissioner, informed us by letter that the West German statute makes no distinction between foreigners and German nationals.[22]

There are no sectoral provisions in the West German statute.

Finally, we would note that the Federal Republic of Germany acceded to the OECD Guidelines on September 23, 1980. It signed the European Convention on January 28, 1981, and ratified it on June 19, 1985. This Convention came into force on Germany territory on October 1, 1985.

We may conclude with respect to this group of European countries that personal data concerning Canadians and stored on the territory of any of these three countries are protected on the same basis as data relating to their nationals. This is, as we have said, consistent with their ratification of the European Convention.

---

[19] For a more detailed picture of the German legislation, see in particular Eckhardt K GOURAS, "The Reform of West German Data Protection Law as a Necessary Correlate to Improving Domestic Security", [1986] 24 *Columbia Journal of Transnational Law*, 597.

[20] Joke DeHOUWER. *The Transborder Flow of Personal Data (A Comparative Study of International and National Regulations)*, Vrije Universiteit Brussel, October 1989, Appendix A, Germany, p 2.

[21] Ibid, pp 2 to 4.

[22] See the text of the letter appended to this report.

1.4 *The United States of America*

Before starting our description of the legal protection of personal data offered in the United States of America (1.4.3), we thought it advisable to quickly examine the general framework (1.4.1) and sources (1.4.2) of this protection.

1.4.1 *General framework of protection*

United States legislation represents another type of approach to personal data protection. Personal data are considered as a particular category of a broader legal phenomenon known as "privacy". A wide variety of measures have been implemented to protect privacy, or non-intrusion into an autonomous and reserved sphere belonging to the individual, who not only possesses this right but is also its principal defender.

This enables us to understand the peculiar nature of the protective measures adopted, which are directed primarily against government intrusion, this being considered the primary and principal potential threat to privacy. To some extent, the realization of the disproportionate resources of the two sides created the need to limit and specify the ways in which the government could intervene in private matters, something against which it would be difficult for an individual to be effectively forearmed. However, in the case of private dealings, the general scheme of the law in the United States prefers to leave matters to be freely bargained between the parties.

We will, therefore, note a clear distinction between the legal treatment of situations in the public sector, which is widely regulated, and the private sector, where there is much less regulation. In the private sector, legislatures intervene only to correct those imbalances that are too flagrant and which could not be prevented by the process of mutual agreement. This also explains why the private sector legislation is designed to protect the weakest parties. This legislative approach is characterized by the enactment of legislation described as "fair information practice". This legislation is not designed primarily to protect personal data specifically, but rather to create honest and correct information practices that are left to the defence of the individuals on whom these rights are conferred.

This approach also explains why we find no general and unique legislation protecting personal data, but rather a host of scattered provisions designed solely to limit potential intrusions upon privacy by various governmental or private parties. The American approach to privacy protection is sectoral rather than global, personal data being only one component of privacy.

Finally, this approach complicates our task because we cannot give a simple answer to the question of the level of protection offered by legislation for personal data concerning Canadians for all the United

States. The level of protection will often depend on who has the information and the sector in question. The protection offered will vary depending on what federal or state government organization or what firm in what part of the private sector has the data.

The situation is further complicated by the fact that we also had to ask the question of how each of these specific laws applies to foreigners and, more specifically to Canadians, to determine the degree of protection offered to personal data about them. As we shall see, the application of American legislation to foreigners is a widely debated issue about which there are few certainties. In the public domain, the legislation is known and identifiable. Compliance with the OECD Guidelines, as we have seen, provides us with at least a relatively solid standard of interpretation, if not a complete legal reference. In the private sector, however, this private international law question is not a simple one, depending on the legal nature ascribed by each jurisdiction to transactions involving personal data.

In trade matters, we know that federal jurisdiction prevails in all aspects of interstate commerce (the interstate commerce clause)[23] but this clause is not exclusive. It does not prohibit states from legislating in areas to which Congress has not yet devoted its attention or from legislating in a manner that is not inconsistent with provisions already enacted by Congress or under its authority. Mere knowledge of a federal enactment that could operate to regulate transborder personal data flows would, therefore, still not relieve us of the task of determining whether, in addition to federal enactments, valid state enactments might not also apply to such matters, in addition to the federal enactments.

1.4.2 *Sources of the protection*

We can identify five categories of sources of personal data protection in the United States.

First, with respect to international law, the United States is not to date a party to any convention or treaty on the protection of personal data, although it has indicated that it will comply with the OECD Guidelines which, we believe, cover data about foreigners. However, with respect to the application of the Guidelines in the private sector, the United States chose to implement them by recommending voluntary compliance on the part of private firms. In a letter dated July 1981 to the 100 largest multinational corporations and to 40 trade associations, the U.S. Secretary of Commerce urged them to undertake publicly to comply with the Guidelines. In October 1981 the U.S. Trade Representative reported to the OECD that 98 multinational corporations and 12 trade associations had made such commitments. In June 1982, the total number of public commitments had risen to 157. Although the Reagan administration soft-pedaled these efforts, the process of adhesion and voluntary implementation has probably produced the maximum effect to date that can be expected from this sort of noncoercive encouragement.

---

[23] U.S. Constitution, Art 1, sec 8: "The Congress shall have the power... para 3: To regulate commerce with foreign nations, among the several States, and with the Indian tribes."

A second source of general personal data protection in the United States can be traced to the broad principles set out in the Constitution[24] of the Federation itself, which created an area of privacy where government or state intervention is not permitted:

the First Amendment, which limits the use of information held by the government on individuals, by prohibiting the government from using such information in a discriminatory manner;[25]

the Fourth Amendment, protecting against unreasonable search and seizure, which has been extended to apply to government interceptions of telephone or other conversations;

the Fifth Amendment, permitting a person to refuse to give testimony that could be self-incriminating; and

the Fourteenth Amendment, which limits government use of personal data that could penalize the person by not treating him or her equally[26].

However, except for these last two provisions, in which the text of the Constitution itself uses the expression "any person" rather than "people" or "citizen", it is not clear that foreigners enjoy any constitutional protection before the courts, other than the procedural protections[27].

Moreover, on February 28, 1990, the Supreme Court of the United States delivered a judgment on this question which, in our opinion, may reverse long-standing case law. In U.S. v Rene Martin Verdugo-Urquidez (Sup Crt Feb 28, 1990), it was decided that: "The Fourth

---

[24] The right to privacy is not explicitly expressed in the Constitution, but the courts have found that it is implied by the Constitution, particularly in *Griswold v Connecticut* (S Ct, 1965) 381 US 479, and also in *Whalen v Roe* (S Ct, 1977) 429 US 589.

[25] *Katz v US* (S Ct 1967) 389 US 347; and *Berger v New York* (S Ct 1967) 388 US 41.

[26] Fourteenth Amendment, section I, conclusion: "Nor deny *any person* within its jurisdiction the equal protection of the laws." In context, this passage clearly indicates that foreigners are also covered in so far as, by comparison and interpretation, the initial passage of this Article confers still broader and more generous rights on "All persons born or naturalized in the United States".

[27] *Ashbury Hospital v Case County* ND 326 US 207 (1945): "A corporation is neither a 'citizen of a state' nor a 'citizen of the United States' within the privileges and immunities clause of the Constitution or the Fourteenth Amendment. The Fourteenth Amendment does not deny to a state power to exclude a foreign corporation from doing business or acquiring or holding property within it."

Amendment does not apply to the search and seizure by United States agents of property owned by a nonresident alien and located in a foreign country." This decision certainly has a direct effect on the protection offered to Canadians' personal data held not only in the United States, but also in Canada itself because American agents have now been given extraordinary latitude with respect to personal data concerning foreigners. While it is too early to assess the magnitude of the effects of such a decision on the protection of foreigners' personal data in the United States, we can only hope that this decision will be applied restrictively.[28]

However, this judgment goes well beyond the simple application of the Fourth Amendment, the terms of which had led us to the same conclusion. This judgment goes so far as to dismiss any claim by a foreigner who is not on United States territory to any constitutional protection at all. It states, contrary to what had earlier been considered to be the rule, that foreigners do not fall into the category included in the expression "We the people" that provides the introduction to the Constitution and, accordingly, a foreigner can make no claim whatsoever to be a party to the constitutional pact nor claim the protection that flows from it.[29]

However, we find here some support for the distinction that we made earlier between the terms "people" and "any person" in that the court states: "The language of these Amendments contrasts with the words 'person' and 'accused' used in the Fifth and Sixth Amendments regulating procedure in criminal cases."[30] On the other hand, a little later on, the judgment holds that the same wording in the Fifth Amendment, "No person shall...", does not prevent the Supreme Court from treating citizens and foreigners differently. However, in stating: "If there are to be any restrictions on searches and seizures which occur incident to such American action, they must be imposed by the political branches through diplomatic understanding, treaty, or legislation", this decision invites us to consider the opportunity to protect personal information about Canadians by way of agreement or special legislation.

---

[28] The judgment also explicitly refers to the actions of agents of the United States abroad: "Not only are history and case law against respondent, but as pointed out in Johnson v Eisentrager, supra, the result of accepting his claim would have significant and deleterious consequences for the United States in conducting activities beyond its boundaries. The rule adopted by the Court of Appeals would apply not only to law enforcement operations abroad, but also to other foreign policy operations which might result in 'searches or seizures'. The United States frequently employs armed forces outside this country — over 200 times in our history — for the protection of American citizens or national security. ...Applications of the Fourth Amendment to those circumstances could significantly disrupt the ability of the political branches to respond to foreign situations involving our national interest. Were respondent to prevail, aliens with no attachment to this country might well bring actions for damages to remedy claimed violations of the Fourth Amendment in foreign countries or in international waters." In this respect, we cannot help but think of the recent Panama case and the fate awaiting General Noriega.

[29] Chief Justice Rehnquist, speaking for the majority: "...These cases, however, establish only that aliens receive constitutional protections when they have come within the territory of the United States and developed substantial connections with this country. See, eg. Plyler, supra, at 212 (The provisions of the Fourteenth Amendment "are universal in their application, *to all persons within the territorial jurisdiction...*") (quoting Yick Wo, supra, at 369); Kwong Hai Chew, supra, at 596, n 5 ('The Bill of Rights is a futile authority for the alien seeking admission for the first time to these shores. *But once an alien lawfully enters and resides in this country* he becomes invested with the rights guaranteed by the Constitution to all people within our borders.') (quoting Bridges, supra, at 161 [concurring opinion] [emphasis added])."

A third source of general protection for foreigners' personal data in the United States may be found in certain general provisions of the common law[31]. For example, banks are required to keep their information confidential; doctors, lawyers and, in some circumstances, members of the clergy enjoy a privilege in legal proceedings and must keep confidential any information they have received in that capacity. There are also numerous rules concerning libel that provide a measure of protection for personal data in the United States and may be asserted by foreigners. A majority of states recognize the right to privacy in their common law.[32]

Fourth, personal data may, as anywhere, be protected voluntarily by specific contractual clauses, or by self-disciplinary measures such as codes of ethics or conduct adopted by lawyers, doctors, newspapers and media, hospital administrators and so on. We have also found that increasing numbers of large corporations are using this method.

Finally, in the United States there is a host of general or specific legislation that is designed directly or indirectly to protect personal data, either in general or in the public or private sector. A glance at a list of the most important federal legislation provides an indication of the intensity of legislative activity in this area.[33]

---

[30] "While this textual exegesis is by no means conclusive, it suggests that 'the people' protected by the Fourth Amendment, and by the First and Second Amendments, and to whom rights and powers are reserved in the Ninth and Tenth Amendments, refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community. See United States ex rel Turner v Williams, 194 US 279, 292 (1904) (Excludable alien is not entitled to First Amendment rights, because '(h)e does not become one of the people to whom these things are secured by our Constitution by an attempt to enter forbidden by law'). The language of these Amendments contrasts with the words 'person' and 'accused' used in the Fifth and Sixth Amendments regulating procedure in criminal cases."

[31] Justices Brandeis and Warren, one of whom was ending his career on the Supreme Court, defined this individual right to be left in peace in a famous 1890 article in the *Harvard Law Review*, and suggested that this right be buttressed by legal remedies in privacy torts: civil liability for damages resulting from violation of this right to privacy.

[32] Except for the following states: Minnesota, Nevada, North Dakota, Wyoming. See Smith, Robert Ellis, *Compilation of State and Federal Privacy Laws* 1988, p 29.

1.4.3 *Legislative protection*

Having said this, we would note that there is no general legislation that would protect all personal data in the United States in both the public and private sectors. However, there may be specific legislation governing personal data in certain specific situations in both public and private sectors.

An example is federal computer crime legislation (Computer Fraud and Abuse Act)[34] which indirectly criminalizes certain activities involving personal data when such data are stored or processed using computers. This Act criminalizes unauthorized access to a computer system. It is also a civil tort to access a computer system without authorization and to obtain information from such a system if state borders are crossed in so doing.

This legislation, covering all personal data that are transmitted by computerized transborder flows, is clearly within our subject area. Entering or accessing a computerized transborder data flow without authorization is an offence. Trafficking in passwords or methods of accessing such systems or flows is also an offence that the various government services are required to take action to prevent (PL 100-235, enacted in January 1988).

Federal computer crime legislation now covers cellular telephones, electronic mail and electronic data transmissions, it being an offence to intercept them (Electronic Communications Privacy Act of 1986, PL 99-508, amending 18 USC 2511, 3117, 2701, 3121, inter alia). In so far as personal data concerning Canadians being transmitted by computer may be the subject of such crimes, this might be said to be a form of protection.

We did not identify any American state that had general personal data protection legislation covering both public and private sectors. However, several pieces of state legislation that are not specifically designed to protect personal data nonetheless offer some protection, generally through the general protection afforded private property, the integrity of the person or what is referred to as "privacy". We will now examine each of the six states which, according to the results of our study, show a high level of occurrences as recipients or transferees of personal data flows from Canada. Despite a lower occurrence rate, we have also added Texas because of the very large volume of data transferred there.

---

[33] *The Wiretapping Act* of 1968: 18 USC 2510.
The Fair Credit Reporting Act of 1970: 15 USC 1681(a)(4).
The Privacy Act of 1970: 5 USC 552a.
The Right to Financial Privacy Act of 1978: 12 USC 3422-3401.
The Electronic Communications Privacy Act of 1986: 18 USC 2701-2709, and 321 et seq.
The Computer Security Act of 1987: 15 USC 271-278h.
The Computer Matching and Privacy Protection Act of 1988: PL 100-503, 102 Stat 2507.
and also:
The Freedom of Information Act: 5 USC 552.
The Cable Communications Policy Act of 1984: 47 USC 551.
and so on.

[34] 18 USC Ch 47, Sec 1030, as amended by PL 99-474 in 1986 and by PL 100-235, 101 Stat 1725, Jan 8, 1988.

NEW YORK

The first Article of the State Constitution provides: "the right of the people to be secure against unreasonable interception of telephone or telegraph communications shall not be violated..." (Art I, sec 12, NY Constitution, 1938); and any violation constitutes a tort for which damages may be sought (NY Civ Rights Law, sec 50 (McKinney)). This Article has also been interpreted to cover computer flows and to provide indirect protection to foreigners to the extent that the New Yorkers they are dealing with enjoy such protection.

Improper and unauthorized entry into a computer system containing medical or confidential information is an offence ("computer trespass"), as is unauthorized copying or falsification of computer data. The law also has extraterritorial effect in that it provides for the prosecution of a person who, without authorization, takes data in the State of New York from another state (NY Penal Law, Art 156).

Some categories of data are also protected in both the public and private sectors in New York State. These are primarily data found in employment and medical records, which cannot be disclosed without the consent of the employee, patient or doctor (Pub Off Law sec 89(2)(b)(i)). No employer may require, suggest or knowingly permit an applicant or an employee to submit to a psychological test or lie detector test. An employer may not use the results of such a test (NY Labor Law, sec 733), nor require fingerprinting as a condition of employment (NY Labor Law, sec 201-a).

CALIFORNIA

Here again, the State Constitution provides general protection for personal data: "All people are by nature free and independent, and have certain inalienable rights among which ... pursuing and obtaining safety, happiness and privacy" (Art 1, sec 1, Cal Constitution, Nov 1972). While it is not clear that the expression "people" also covers foreigners, the affirmation of the protection of privacy in the State Constitution is to be used in interpreting any other legislative enactments that may themselves apply directly or indirectly to foreigners.

California also has a general statute requiring employers in the public and private sectors to permit an employee to inspect all records and personnel files concerning him or her within a reasonable time, upon request. Letters of reference and records of criminal investigations are excluded. The records must be available at the place where the employee is required to report for work (Cal Labor Code, sec 1198.5 and Cal Education Code, secs 24317 and 92612).

With respect to the use of computers to transmit data, California offers still more specific protection that covers personal data to some extent. It is an offence to enter a system or computer network maliciously with intent to defraud or extort money or services or to access a system maliciously in order to alter, erase, damage or destroy any computer system, network, program or data (Cal Penal Code, sec 502). Publication of a personal identification number (PIN), password, access code, debit card number or bank account number is also a crime (Cal Penal Code, sec 484j).

FLORIDA

This state also has a constitutional provision that may provide some general protection for personal data: "Every natural person has a right to be left alone and free from governmental intrusion into his private life except as otherwise provided herein. This section shall not be construed to limit the public's rights of access to public records and meetings as provided by law" (Art 1, sec 23, Fla Constitution: approved by the 1980 electoral referenda). The wording of this Article leads us to believe that Florida provides such protection without regard to the status of the person who is the subject of the data.

We are supported in this interpretation by Article 1, section 12 of the same Constitution, which reserves other important constitutional rights, such as the protection against unreasonable searches and seizures, to "the people" rather than to "every natural person": "The right of the people to be secure in their persons, houses, papers and effects against unreasonable interception of private communications by any means, shall not be violated." This interpretation *a contrario*, which is consistent with the reasoning adopted by the Supreme Court in the Verdugo-Urquidez case, cited above, would permit us to assert that foreigners would receive specific protection here. This is particularly important in that this right is accompanied by the legal remedies that are necessary for the protection of privacy (Fla Stat Ann secs 770.05 to 770.07).

As in the other states examined above, there is a general statute in Florida on computer crime: protection of intellectual property, computer equipment and computer users. This legislation prohibits deliberate modification, destruction and deliberate disclosure of certain data (Fla Stat Ann sec 815.01), so indirectly protecting data concerning foreigners.

WASHINGTON

The Constitution of Washington State also contains a general provision that applies to everyone: "Right to privacy: No person shall be disturbed in his private affairs, or his home invaded, without authority of law" (Art 1, sec 7, Wash Constitution, 1889, as amended), as well as provisions concerning computer crime (Wash Rev Code Ann sec 9A.48.100 (1984)), that indirectly cover data concerning foreigners.

Here again, general provisions common to the public and private sectors protect data in employment records and also confer a right to obtain access and make corrections (Wash Rev Code Ann sec 49.12.250), except when a person is applying for public employment for the first time.

MICHIGAN

Although we did not identify any constitutional legislation in Michigan, there is legislation of general application that covers both the public and private sectors and which is designed to protect personal data.

Employees have a right to obtain access and make corrections to their employment records (Mich Comp Laws Ann sec 37.201). Finally, there is general legislation on computer crime (Mich Comp Laws Ann sec 752.791).

MASSACHUSETTS

Massachusetts, as well, has general legislation that protects privacy and, accordingly, personal data: "A person shall have the right against unreasonable, substantial or serious interference with his privacy" (Mass Gen Laws Ann ch 214, sec 1B) and the courts may award damages where the right is infringed (sec 3A). The concept of property in the legislation includes "electronically processed or stored data, either tangible or intangible (and) data while in transit" (Mass Gen Laws Ann ch 266, sec 30[2]).

General legislation covers employment records. On written request, an employee in the private or public sector may obtain a copy of his or her personal records and enter comments in the record if it contains incorrect information.

The employer is liable if information that it knows is false appears in the record (Mass Gen Laws Ann ch 149, sec 52C). Any employment form must state: "It is unlawful in Massachusetts to require or administer a lie detector test as a condition of employment or continuous employment" (Mass Gen Laws Ann ch 149, sec 19B, amended in 1986). A court may award treble damages in such cases. An applicant for employment may refuse to disclose information on his or her criminal record (Mass Gen Laws Ann ch 151B, sec 4, para 9).

Similarly, school records are to some extent protected by the right of access (Mass Gen Laws Ann ch 71, secs 34A, 34E and 34D), while there is medical records protection legislation entitled the patients' charter of rights (Mass Gen Laws Ann ch 111, sec 70E, and ch 123, sec 36, and ch 149, sec 19A). In January 1990, bills on computer crime were tabled (Senate Bills No 309 and 214). They follow the bill tabled in April 1989 that criminalizes unauthorized access to a computer or to a data bank (House Bill No 4337).

TEXAS

Our study showed that large volumes of personal data flows are transmitted to Texas, although few respondents reported this state as a destination. However, we did not identify any general legislation that would protect personal data transferred from Canada. All that we found was legislation relating to lie detector tests, which are permitted if the employee voluntarily submits to the test and is informed of the results (Tex Rev Civ Stat Ann art 4413(29cc)). As well, a Computer and Computerized Crime Act came into effect on September 1, 1989, "to define terms and criminal activities encompassing computer crime".

1.5 Other countries

Generally speaking, a majority of the other countries studied have no legislation protecting personal data, and they referred us to the general protection that was referred to as "contextual" in *L'Identité piratée*: the constitution, civil code, general legislation on commerce and contracts and, potentially, national or international charters of rights.

Before receiving the results of our study, we did a prospective study of all relevant legislation in all these countries, summarizing the results in Part One in the presentation on methodology and the state of the question. Information is available but, given the results of the study, there is no point in dwelling on the protection offered by these various countries because occurrences and volumes of transborder personal data flows from Canada, at least so far as our respondents are concerned, are quite minimal. Furthermore, to discuss them would almost require analyzing the records of each respondent.

Four countries (Australia, Japan, Italy and Hong Kong) stand out in our study as destinations for significant personal data flows. None of these countries has general legislation covering both public and private sectors. Australia acceded to the OECD Guidelines on December 10, 1984, but it has not ratified the European Convention. In this respect, it might be useful to note that Article 23 of the European Convention authorizes the adhesion of non-member States of the Council of Europe. Japan, whose legislation covers only the public sector, adopted the OECD Guidelines on September 23, 1980, but has not yet signed the European Convention.

In Italy, the legislative situation could not be simpler: there is no specific legislation relating to personal data protection. Draft legislation on the question[35] (Mirabelli and Martinazoli Bills) has been tabled but it is still at the discussion stage.

---

[35] OECD, *Situation actuelle et tendances de la protection de la vie privée dans la zone de l'OCDÉ*, Paris, OECD, DSTI/ICCP/88.5, p 14.

In Hong Kong, it appears that the Tiananmen Square events and the growing development of nominative data protection legislation in Western Europe led the government to adopt a personal data protection law. The government of Hong Kong established a committee to study foreign legislation on this subject and to propose legislation for 1991. According to the committee, this legislation should cover the public sector and certain segments of the private sector[36] (insurance, credit agencies and so on).

This completes our examination of the overall situation with respect to legislative protection in the major countries of destination as identified by our study. We have examined the broad types of protection in Europe, the United States of America and certain other countries.

We will now examine the countries of destination and the legal protection offered in the public sector (2) and the private sector (3). Then, we will examine the results of our survey by groups of sectors for our public sector respondents (4), before doing the same for the private sector (5).

---

[36] "Hong Kong. Privacy Law Drafting Committee Formed", (1990) 13 TDR 25.

2 Countries of destination reported by public sector respondents

2.1 Results of the survey

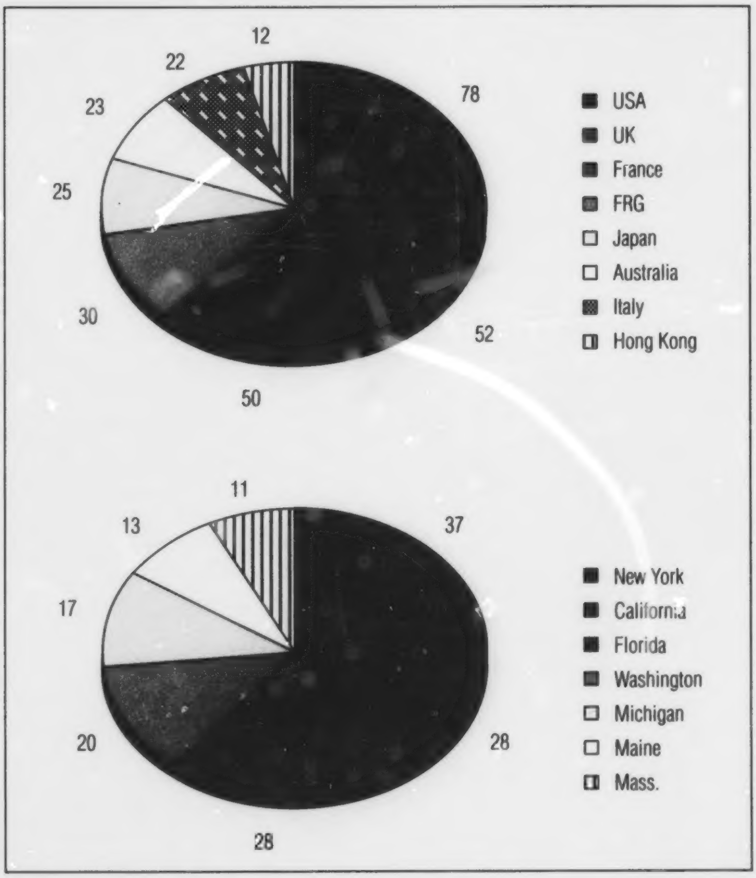
When we isolate the questionnaires of the public sector respondents, we find very little difference from the overall results. The United States is still in the lead by far among the countries of destination, with a wide variety of destinations. If our criterion to determine significance is the threshold of 1% of respondents, we find substantially the same countries and the same American states. In fact, the only difference visible in Table 2-1 is the disappearance of Texas and the appearance of Maine. In this table, the asterisk (*) indicates an American state.

Table 2-1
Significant destinations in terms of occurrences, public sector

Country/state	Occurrences	Occurrences /N of respondents (%)
United States of America	163	15.16
United Kingdom	82	7.63
France	64	5.95
Federal Republic of Germany	50	4.65
* New York	37	3.44
Japan	35	3.26
* California	28	2.60
* Florida	28	2.60
* Washington	20	1.86
* Michigan	17	1.58
Australia	15	1.40
Italy	15	1.40
* Maine	13	1.21
Hong Kong	12	1.12
* Massachusetts	11	1.02

We also find only a slight change in the ranking of the American states but that, when there is a change, the states tend to drop in rank (New York and Massachusetts, while Texas disappeared from the list) and the other countries tend to rise in rank (FRG, Italy and Hong Kong). However, there are exceptions: Michigan and Maine, two states on the Canadian border, moved up. This situation may be explained by the fact that some Canadian residents work on the other side of the U.S. border or reside temporarily in an American state, these lifestyle factors requiring that some data be transmitted abroad by public sector organizations.

Graphic 2-1
Countries and American states of destination, public sector



These figures could, however, cause us to lose sight of an important aspect of the real situation. Although the primary destination of transborder personal data flows is the United States, public sector respondents transmit proportionately much less personal data to that country while transmitting more than private sector respondents to most other destinations.

To illustrate this phenomenon, Table 2-2 sets out a list of the countries for which a larger proportion of public sector than private sector respondents report transferring personal data. In this table, the rank of each country or American state is based on the difference between these two percentages. The asterisk (*) indicates an American state.

It will be noted from this table that there are four European countries among the top five on the list, while the three border states, Maine, Michigan and Washington, appear in fourth, sixth and seventh place.

The difference in the case of eighth place Japan is almost negligible. This means that the predominance of the United States as a country of destination is less in the public sector than in the private sector.

Table 2-2
Proportion of public sector/private sector respondents

Country/state	Public sector (%)	Private sector (%)	Difference (%)
1 - Fed Rep of Germany	4.65	2.18	+2.47
2 - France	5.95	4.51	+1.44
3 - United Kingdom	7.63	6.40	+1.23
4 - * Maine	1.21	0.29	+0.92
5 - Italy	1.40	0.83	+0.67
6 - * Michigan	1.58	1.16	+0.42
7 - * Washington	1.86	1.45	+0.41
8 - Japan	3.26	3.05	+0.21

The figures we have analyzed to this point for the public sector relate only to the number of occurrences. If we now analyze transfers of very large volumes of personal data, we find that relatively few public organizations are involved in such types of transfers. Table 2-3 identifies the types of public organizations involved in personal data transfers with volumes of more than 10,000 during the last year or during the last five years. It also indicates the number of persons (clients or others) affected by the data disclosed and the destinations of the transfers. It should be noted that no public sector respondent reported in response to subquestion 3(e) that the total number of persons affected by personal data held abroad because of such transfers exceeded 100,000 persons. In this table, the notation (o) indicates that the number refers to "other" persons.

Table 2-3
Destination of very large volumes, public sector

Type of organization	Number of clients/1 year	Number of clients/5 years	Destination
HEALTH/SOCIAL SERVICES			
Hospital		15,000	Florida
GOVERNMENT			
Department	30,100	125,000	USA
Public Organization		28,000	USA
Department		10,690 (o)	more than 20 countries
Department		10,000	more than 20 countries

We note that only five public organizations transferred large volumes of personal data. They represented only 0.47% of the public sector respondents (5/1075), or 2.37% of the respondents in this sector who reported transferring personal data (5/211). Our first comment would be to note that, except for one case, these transfers all concerned clients or rather, because these are organizations in the public sector, persons under the administration of the organization. The one exception may be a result of poor comprehension of the question by the respondent. It is difficult to see how a public organization, particularly a federal department, could transfer information about Canadian citizens or residents who were not also under the department's administration.

The second comment we would make is that when there are large volumes of personal data transmitted abroad by the public sector, there are also multiple destinations. There are exceptions to every rule: Florida is the only destination for a hospital that transferred personal data about more than 15,000 clients during the last five years. We will return to these cases in our sectoral analysis.

2.2 *Legal protection*

We have now seen the occurrences and volumes of data transferred by public sector exporters of personal data. Knowing that Canadian exporters send personal data flows primarily to organizations in the same sector as themselves, we shall now analyze the specific legal protection in the public sector in general that is offered in the countries of destination. We will retain the same group typology for this purpose as was used earlier; that is, Europe first (the United Kingdom, France and the FRG), followed by the United States with the main states of destination, and then the other countries (Japan, Australia, Italy and Hong Kong).

2.2.1 *Europe*

For the three European countries that are major destinations for personal data flows from Canada, there is nothing to add to what was said earlier in our analysis of the various statutes specifically governing both the public and private sectors. On the other hand, we did not identify any legislation in these three countries that would apply specifically to the public sector.

2.2.2 *United States*

For the United States, we must analyze the relevant public sector legislation in turn by level: first, federal, because such legislation takes precedence over state legislation and second, because of relevant state legislation in the public sector. This analysis for the United States in general and New York in particular has already been done in the GRID publication cited above[37]; we do not think it necessary to restate it in full here and would refer the reader to that text. We will examine here the legislation governing the records held by governments, first at the federal level, and then in the states that appear in Table 2-1.

1. Federal legislation

Apart from the constitutional provisions that we have examined, and the various general sources of protection for personal data, the Privacy Act of 1974 (5 USC 552a) is the principal legislation in this domain in terms of the public sector in general.

This law adopts the principle of the confidentiality of records and the right of access. It places some limits on federal actions with respect to the handling of personal data contained in or sent to government files. The object of the legislation is to ensure that data about a physical person by which he or she could be identified (5 USC 552a (a) 4) and which are held by the federal government and its various branches are protected, and to permit citizens who are the subjects of such data to have access to it. The right of access is reserved to citizens only and does not extend to foreigners (5 USC 552a (a) 2). However, the other obligations of confidentiality and secure management of records that apply to federal public institutions apply regardless of the nationality of the individuals about whom the institutions hold personal data.[38]

This law does, however, contain a number of exclusions and exemptions: for example, for military matters (veterans: 38 USC 3006) or national security (5 USC 552a). In addition, disclosure of federal administration files is permitted in a number of cases, including:

- locating defaulters on alimony payments: 42 USC 653;
- comparing or identifying federal social benefits recipients: 42 USC 611 and also 42 USC 111;
- detecting fraud: 42 USC 1320b-7(a) and (c);
- exchanges of information about child adoptions: 42 USC 51;3(b)3.

The Paperwork Reduction Act of 1980 requires that the Office of Management and Budget create the Office of Information and Regulatory Affairs to coordinate the development and implementation of federal policies concerning, among other things, records management and confidentiality, information-sharing among agencies and the acquisition and use of automated data processing. The

---

[37] LAPERRIÈRE, René, and PÉLADEAU, Pierrôt. *Le droit sur la protection des renseignements personnels: Étude sur les bases privées de données à caractère personnel en droit canadien, comparé et international*. Montreal, 1986, SOQUIJ, pp 9 to 61.

[38] This statement would require some modification if we were dealing with a complete bank of personal data that concerned only information about persons who were not American nationals or permanent residents.

Office establishes guidelines with respect to privacy protection, providing the administration with the advice and appropriate framework to comply with the Privacy Act (44 USC 3501).

2. State legislation

Several states have adopted measures with respect to matters under their jurisdiction that are similar to federal privacy legislation and which meet the objectives of confidentiality and freedom of information, protect electronic funds transfers and, frequently, create offences relating to computers or wiretapping.

In 1980, the National Conference of Commissioners on Uniform State Laws adopted a Uniform Information Practices Code, codifying the principles of freedom of information and access by individuals to their personal records. This dual principle of freedom of information coupled with privacy protection, is centred on an exception to the free flow of information insofar as it relates to files concerning identifiable subject individuals. In other words, all records are accessible except those containing personal data, the latter being accessible only to the individual concerned, who may check the accuracy of the records and have the opportunity to enter comments. However, it is noted that we are seeing a resurgence of concerns about the security of information and the extension of the fields and policies that are not subject to freedom of information.[39]

NEW YORK

This state has general legislation that protects personal data in the public sector: the Personal Privacy Protection Law (NY Pub Off Law 6A, sec 91). This statute, the principles of which are close to those of the federal statute, protects the confidentiality of records and grants access to public archives and a right of correction (sec 92). The various administrations must keep consultation registers and register data banks. The terms of this legislation extend its application to any person concerned and, accordingly, to non-citizens. This statute is the companion to the Freedom of Information Law (NY Pub Off Law 6 Sec 84).

CALIFORNIA

In addition to the State Constitution which, as we have noted, protects the right to privacy, some provisions of California statutes relate directly to the protection of personal data held by public service in general. In that these statutes impose obligations on public institutions, foreigners may benefit indirectly even though they may not always directly enjoy the personal rights of access and correction set out therein.

---

[39] See: *Security and Confidentiality of State's Informational Assets Act*:
- for California: (ch 364, Laws of 1989) in effect since January 1990;
- for Florida: (ch 14, Laws of 1989) in effect since October 1, 1989;
- for New York: Assembly Bill Nos 1206 and 1207 of January 1989.

Freedom of information and the right of access to public records are affirmed in the Public Records Act (Cal Govt Code sec 6250 et seq). The State's Fair Information Practices Act grants citizens a right of access and correction with respect to records concerning them. There are conditions on the disclosure of this information that are specific with respect to universities and the police. In addition, in the event of a violation of privacy, this law permits prosecution of any person who intentionally discloses personal information that he or she knew was obtained from the state or a federal agency (Cal Civil Code sec 1798, as amended in 1979). Moreover, files on library consultation are confidential (Cal Govt Code sec 6254(j)) but those relating to motor vehicles are not (Cal Vehicle Code sec 1810).

In the area of criminal records, an individual who is or has been convicted has a right to access and correct information in his or her file (Cal Penal Code sec 11121-26). If a person is acquitted, the judge may order the record sealed and later destroyed (Cal Vehicle Code sec 1810). An individual's arrest record cannot be considered by employers with respect to job applicants or by public agencies with respect to an individual seeking a licence, certificate or registration (Cal Labor Code sec 434.7 and Cal Bus and Prof Code sec 461). Nor can automobile insurers do so (Cal Ins Code sec 11580.08).

FLORIDA

Florida, too, has almost the complete range of the measures generally available in the United States to protect personal data in public records. As elsewhere, this is a dual protection: confidentiality of records concerning identifiable persons and a right of access to public records.

Each state agency must ensure that information is secure. For this purpose, they must regularly analyze risks, disclosure policies, security investigations and the precautions necessary with respect to data processing (Fla Stat Ann sec 282.318). A recent statute, which came into effect in October, 1989 (ch 14 Laws of 1989), embodied this concern with respect to the security and confidentiality of public records. A new statute (The Information System Disaster Recovery Act: House Bill No 1336-4 April 1989) further reinforces this concern. Each state agency must also purge its publication mailing lists twice a year, by providing the people on such lists the option of continuing or ceasing to receive publications (Fla Stat Ann sec 283.28).

There is a statute respecting freedom of information and access to public documents: the Public Records Law (119.01 et seq); however, it contains certain exceptions, like lists of social assistance recipients, which cannot be used commercially (Fla Stat Ann sec 409.355(2)(a)), and voters lists (Fla Stat Ann sec 98.211(1)) or library records unless a court specifically orders otherwise (Fla Stat Ann sec 257.261).

Any individual may inspect, dispute and have amended the information contained in his or her criminal record and may also require that all recipients of the original record be notified of the changes made. Some information may be deleted from records after acquittal or after a certain period of time (Fla Stat Ann sec 901.33 and sec 943.056). It is illegal to discriminate with respect to public employment on the basis of prior convictions unless they relate directly to the position in question (Fla Stat Ann sec 112.011).

Of course, the rights of access and control thereby conferred do not all apply to foreigners; however, foreigners benefit indirectly from the structures and processing methods relating to the protection and confidentiality of personal data in place in public institutions.

WASHINGTON

In Washington State the Governor, after consulting advisory committees on data processing, is empowered to establish policies on government data processing. This includes the establishment of "Standards and regulations to establish and maintain the confidential nature of information insofar as such confidentiality may be necessary for individual privacy and the protection of private rights in connection with data processing and communications" (Wash Rev Code Ann sec 43.105.040(4)). Among these is the rule that prohibits all confidential or privileged data held by the state from being processed in a single bank (Wash Rev Code Ann sec 43.105.070).

In addition, the Public Access to Records statute (sec 42.17.290 and 42.17.310) confirms the right of access to information, although neither voters lists (Wash Rev Code Ann sec 29.04.100) nor tax records may be used for commercial purposes. School records in the public schools are not accessible to the public (Wash Rev Code Ann sec 42.17.310).

Criminal records assembled under the authority of the state are considered to be privileged and must, therefore, be treated as confidential (Wash Rev Code Ann sec 43.43.710). An individual may ask the court to have his or her arrest record destroyed after discharge or acquittal (Wash Rev Code Ann sec 43.43.730). Unauthorized use of a criminal record constitutes a criminal offence (Wash Rev Code Ann sec 43.43.810).

Here again, these rules for the management of public records apply only indirectly to foreigners but, nonetheless, they offer a certain degree of protection.

MICHIGAN

We did not identify any general legislation in Michigan concerning the confidentiality of personal data held in the public sector in general. There is, however, some legislation concerning individual records such as library (Mich Comp Laws Ann sec 397-603) or arrest records (Mich Comp Laws Ann sec 28.243), to which employers may not have access (Mich Comp Laws Ann sec 37.2205a).

MASSACHUSETTS

As we have noted, Massachusetts legislation contains the following general statement: "A person shall have the right against unreasonable, substantial or serious interference with his privacy" (Mass Gen Laws Ann ch 214, sec 1B). Two statutes, Open Records (sec 66:10) and Fair Information Practices (secs 66A.1 et seq), provide a right of access to public records.

In the public sector this right amounts to an obligation on each government service to designate an individual as responsible for each personal data system and to establish rules concerning access, individual disputes and corrections. Each personal data system, whether manual or automatic, must be registered with the Secretary of State (Mass Gen Laws, Ann ch 66A sec , as amended in 1976 and 1977). Moreover, library records (Mass Gen Laws, Ann ch 4, sec 7 definition 26th, subsec K), tax information (Mass Gen Laws Ann ch 62, sec 32 and sec 58A) and criminal records, are confidential although the persons concerned do have a right of access (Mass Gen Laws Ann ch 276 sec 100 A-C and Mass Gen Laws Ann ch 6, secs 167 to 178).

MAINE

A general statute, the Maine Freedom of Access law (sec 1-401 et seq) states that access must be given to information contained in records in the public sector. Other specific statutes guarantee the confidentiality of personal data held in administration records: in tax matters (Me Rev Stat Tit 36, sec 5340); library records (Me Rev Stat Tit 27, sec 121); medical records (Me Rev Stat Tit 5, sec 554); public sector employment records (Me Rev Stat Tit 5, sec 554 and sec 7071); and criminal records. Almost all of these statutes provide a right to access and to make corrections (Me Rev Stat Tit 16, secs 611 and 620), which is normally reserved to citizens only.

This state has even created a specific agency, the Bureau of Central Computer Services, which is responsible for developing rules for the security of and maintaining the confidentiality of information (Me Rev Stat Tit 5, sec 1851). In addition, there is a general provision concerning privacy protection and the creation of a criminal offence for breaches thereof:

A person is guilty of violation of privacy if, except in execution of a public duty or as authorized by law, he intentionally:

A Commits a civil trespass on property with the intent to overhear or observe any person in a private place; or

B Installs or uses in a private place without consent of person entitled to privacy therein, any device for observing, photographing, recording or broadcasting sounds or events in that place, or

C Installs outside a private place without consent, any device for hearing sounds that would not ordinarily be audible.

(Me Rev Stat Tit 17-A, sec 511)

A new crime has just been created: "invasion of computer privacy" (Me Ch 620, L 1990 (HB 462), enacted on February 23, 1990).

2.2.3 *Other countries*

The other countries to which significant flows are exported by Canadian public sector organizations are primarily Australia, Japan, Italy and Singapore. We have already seen that in Italy there is no legislation respecting the protection of personal data in the public sector; nor does Singapore seem to have such legislation.

AUSTRALIA

The Australian privacy legislation was enacted in 1988 and came into force on January 1, 1989. This Act covers only the public sector; i.e., organizations under federal jurisdiction (Commonwealth agencies).

This Act contains specific provisions relating to tax file numbers that are assigned to each person who has ever filed an income statement. In addition, the Privacy Commissioner has the power under section 27(e) to write guidelines concerning specific sectors of the public administration. Such guidelines must be consistent with the general principles of the Act. However, they have only moral force.

There is no specific provision in Australian legislation relating specifically to the application of the law to personal data concerning foreigners.

JAPAN

The Japanese Parliament enacted a personal data protection law in December 1988. The Japanese statute applies only to the public sector and covers only automated indexes. It contains no provision respecting transborder personal data flows. There is nothing in the statute to indicate whether it also protects nominative data concerning foreigners. The Japanese Parliament has not to date enacted any sectoral provisions.

3 Countries of destination reported by private sector respondents

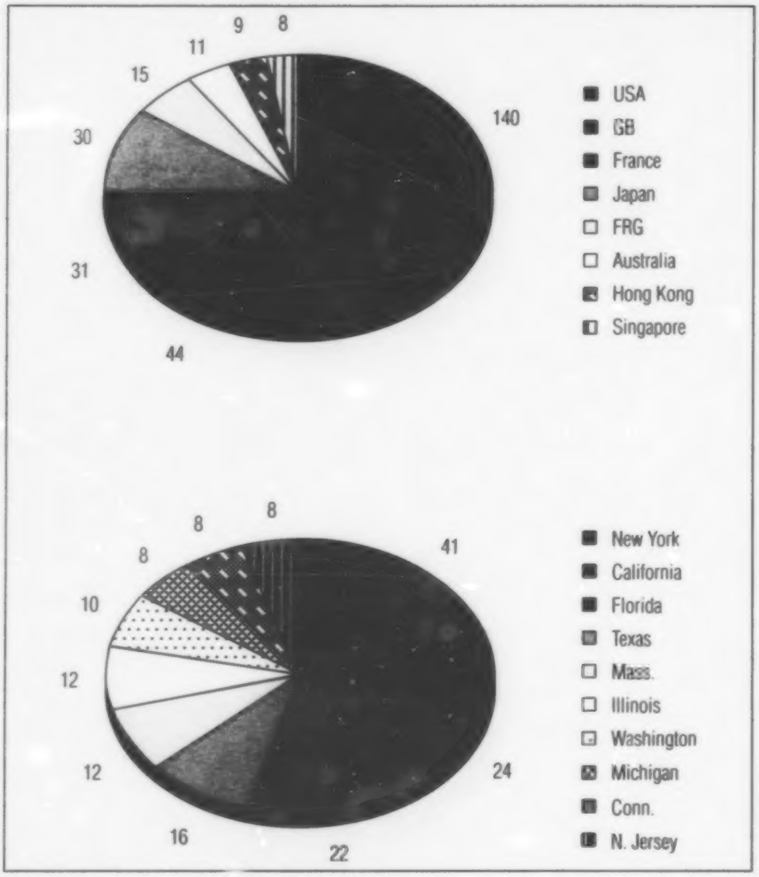
3.1 Results of the survey

We return here to our conclusion that private sector respondents transmit personal data to the United States more frequently than to other jurisdictions. If we again take the criterion for significance used until now in this Part (i.e., that at least 1% of private sector respondents must have transmitted data to a single destination), we find the same trend as in the public sector. In Table 3-1, the asterisk (*) indicates an American state.

Table 3-1
Significant differences in terms of occurrences, private sector

Country	Occurrences	Occurrences /N of respondents (%)
United States	140	20.35
United Kingdom	44	6.40
* New York	41	5.96
France	31	4.51
* California	24	3.49
* Florida	22	3.20
Japan	21	3.05
* Texas	16	2.33
Federal Republic of Germany	15	2.18
* Massachusetts	12	1.74
* Illinois	12	1.74
Australia	11	1.60
* Washington	10	1.45
Hong Kong	9	1.31
* Michigan	8	1.16
* Connecticut	8	1.16
* New Jersey	8	1.16
Singapore	8	1.16

Graphic 3-1
Countries and American states of destination, private sector



Our first observation is that, of the 18 destinations to which more than 1% of respondents transferred personal data, 10 were American states. If we compare the list of countries and states found in Table 3-1 with the list in Table 1-4, we find that Connecticut, Illinois, New Jersey and Singapore are added. The relative weight of the American destinations increases considerably, 20.35% of private sector respondents who reported that they engage in transborder personal data flows transmitting such data to the United States. Another jurisdiction that did not appear in earlier tables appears here: Singapore. This fact is attributable mainly to the associations group, something to which we will return in our sectoral analyses. Italy, on the other hand, has dropped from the list.

The second observation we would make is that the American states have risen in rank in comparison to Table 1-4 while the other countries have fallen. No fewer than eight states have moved up (New York, California, Florida, Texas, Massachusetts, Illinois, Connecticut and New Jersey) while four countries (France, Japan, the Federal Republic of Germany and Australia) and two American states (Washington and Michigan) have moved down.

There is, therefore, a much more marked difference between the results for private sector respondents (Table 3-1) and for all respondents (table 1-4) than there was between the results for the public sector (table 2-1) and for all respondents (table 1-4). The reason is simply that the relative weight of the private sector respondents (690 respondents) is much less than that of the public sector respondents (1,073 respondents).

Table 3-2
Proportion of respondents in the private sector/public sector

Country/state	Private sector (%)	Public sector (%)	Difference (%)
1 - United States	20.35	15.16	+5.19
2 - * New York	5.96	3.44	+2.52
3 - * Texas	2.33	0.56	+1.77
4 - * Illinois	1.74	0.28	+1.46
5 - * Connecticut	1.16	0.00	+1.16
6 - * New Jersey	1.16	0.09	+1.07
7 - * California	3.49	2.60	+0.89
8 - * Massachusetts	1.74	1.02	+0.72
9 - Singapore	1.16	0.47	+0.69
10 - * Florida	3.20	2.60	+0.60
11 - Australia	1.60	1.40	+0.20
12 - Hong Kong	1.31	1.12	+0.19

The figures shown here may be compared to the results of a 1988 GRID study to which we have already referred: among private sector respondents alone, 20.14% reported transmitting personal data to the United States compared to 20.35% in this study. Connections between Canadian private firms and their American counterparts are very strong. It is not surprising to find that their responses in the two studies were identical.

The list of countries and states where there is a higher proportion of private sector respondents than public sector respondents again confirms the predilection of the private sector for the United States.

In table 3-2 we find eight American states, apart from the United States as a national entity, while there are only three other countries, all of which are in the Pacific region. In addition to being few in number, these countries and, particularly, Australia and Hong Kong, show very small differences in comparison with the differences for American states.

We could suggest at least three hypotheses concerning the absence of any European countries in this table. The first would be that economic relations between private Canadian firms and their European counterparts are much less significant than political relations between Canadian and European governments. The second hypothesis would be that private firms avoid transferring personal data to European countries in order to avoid the controls imposed by countries that have enacted personal data protection legislation. The third and most plausible hypothesis is that the economic integration of the North American continent and, particularly, the resulting division of labour (natural resource and manufacturing industries in Canada and service industries in the United States) might explain why the automated processing of nominative data about people residing in Canada is done in the United States. It is likely that these three factors operate concurrently to explain the differences found.

With respect to respondents who report transferring large volumes of personal data, the private sector situation is very different from that which we described for the public sector: 3.5% of private sector respondents (21/688) reported transferring very large volumes, or 12.96% (21/162) of those who report transborder personal data flows in the private sector. The private sector is also distinguished from the public sector in that a very large proportion of respondents in this sector (71.43%) transferred very large volumes of personal data to a single destination while the reverse situation prevailed in the public sector (80% multiple destinations).

3.2 Legal protection in the private sector

Again, we will focus our attention on the three categories of countries identified above: (1) Great Britain, France and the FRG; (2) the United States; and (3) other countries.

3.2.1 Europe

We would note that the legislation of the European countries covers the private sector on the same basis as the public sector. We should provide a few details with respect to France. As we noted, only the private sector is subject to Article 24 of the French statute dealing with transborder data flows.

Article 24 states that prior authorization may be given by the Commission Nationale de l'Informatique et des Libertés (CNIL) for the export of nominative data in order to ensure compliance with the principles of the Law. Article 16 requires private organizations that propose to implement automated processing to file a declaration to this effect with the CNIL, stating that the organization undertakes that the processing will meet the requirements of the Law. Article 19 lists the various points that the firm must include in its declaration. Paragraph 9 of that Article states that it must indicate whether the processing will result in the transfer of nominative data between French and foreign territory, in any form whatsoever. A declaration must be filed with the CNIL respecting any change in any of the factors listed in Article 19. The CNIL may, therefore, make the export of personal data at any time subject to prior authorization because, in theory, it is informed of any such operation.

In examining transborder transfers, the CNIL has adopted the principle of equivalence. This is found in its deliberation No 89-78 of July 11, 1989, in which it makes the export of personal data to Italy, a country that has no personal data protection legislation, subject to an undertaking by the importing organization to comply with the principles set out in the French Law and in the European Convention. Such organization must undertake by contract to follow the fundamental principles of personal data management. Here we have an instance of the application of the principle of equivalence.

It will, therefore, be seen that in the private sector most European legislation protects personal data about foreigners. This is the necessary conclusion reached by interpreting the legislation and the European Convention and, to a lesser extent, the OECD Guidelines.

In this respect, the principle of equivalence plays a central role. The protection accorded to foreigners by the European Convention is quite clearly based on the principle of equivalence. Thus this means that country A is prepared to protect nominative data concerning a foreigner if the latter's country offers equivalent protection to nationals of country A.

The system of minimum standards established by the Guidelines and the European Convention presumes that, to be effective, there is reciprocity in terms of personal data protection. In other words, the theory of a "hard core" is effective only if the fundamental principles of personal data management are laid down in national legislation and, specifically, if it is possible for any individual, regardless or nationality or place of residence, to assert such rights. Otherwise, equivalence would be purely illusory.

As a result, it is possible that Canadian citizens would encounter difficulties if they were to try to exercise their data rights in a foreign country. Section 12(1) of the Canadian Privacy Act limits the right of access to Canadian citizens and permanent residents within the meaning of the Immigration Act, 1976. Extension order No 2 (Privacy Act, Canada Gazette, Part II, Vol 123, No 9, SOR/89-206), adopted under section 12(3), extended this option to any individual present in Canada. A Treasury Board policy dated July 6, 1989, requires that a foreign citizen be present in Canada at the time an application for access is made and at the time a response to such application is received. This residence requirement, temporary though it may be, could perhaps constitute a reason for a foreign national government to refuse to grant Canadian citizens as broad a package of protective measures as it would grant its own nationals.

This assertion must be clarified. It is clear that a country that has ratified the European Convention could not, given Articles 1 and 14 of the Convention, refuse to grant protection to personal data about a Canadian citizen, regardless of Canadian policy in this respect. The provisions of the Convention are strict on this point and appear to admit of no derogation based on the principle of equivalence.

However, this situation may very well arise with respect to countries that have not ratified the European Convention. It is useful to note that only a minority of countries, all of which are members of the Council of Europe, have ratified the European Convention. In other words, countries that have not ratified the Convention could refuse to grant protection to personal data concerning Canadian citizens, arguing that the principle of equivalence is violated in that their nationals do not enjoy the same rights (as those of Canadians) in Canadian territory. Moreover, some countries could refuse to permit the export of personal data to Canada, properly arguing that such data are not accorded protection equivalent to the protection granted by the exporting country. This restriction on the international flow of personal data could be imposed by all countries having nominative data protection legislation, whether or not they have ratified the European Convention. The text of the Convention, like the Guidelines, recognizes the legitimacy of a restriction on transborder data flows based on noncompliance with the principle of equivalence. This situation did not escape Boyle, who wrote in respect of the American statute (Privacy Act of 1974):

> *European nations are concerned that the United States provides less data protection to foreigners than other countries. At the Privacy Act Oversight Hearings, Ronald Plesser, former general counsel to the Privacy Protection Study Commission, stated: "Many foreign countries... require that other countries to whom information about their subjects may be transferred have equivalent levels of privacy protection. The Privacy Act of 1974 is not generally seen as satisfying these requirements for equivalent protection because non-citizens or resident aliens are excluded from its protections".*[40]

The position of Canada on the issue of access may, therefore, have serious consequences both on personal data concerning Canadian citizens recorded abroad and on the export of personal data to Canada.

---

[40] David C BOYLE, "Proposal to Amend the United States Privacy Act to Extend its Protections to Foreign Nationals and Non-Resident Aliens", (1989) 22 Cornell International LJ 285, p 302.

3.2.2 *American legislation*

It must be recalled here that federal legislation may regulate the management of records and indexes in the private sector when the institutions in question are involved in inter-state commerce. On this point, we would refer the reader to the work published earlier by GRID[41] describing the legal protection of personal data in the private sector of the United States. There is no legislation that covers the entire private sector in general in the United States. The same is true of the various American states, none of which has enacted general legislation covering personal data protection in the private sector as a whole. We still find there sectoral legislation and general provisions conferring civil remedies in the event of the violation of privacy rights or the failure to respect the confidentiality of certain data.

We have already referred to legislation in a number of states that directly or indirectly protects personal data in all sectors, both private and public. These were generally statutes concerning the management of employment records, computer crime, medical records or various tests, library records, and so on, this being the case primarily for the states of New York, Florida, Washington, Michigan and Massachusetts. We do not plan to repeat the general discussion set out in section 2.2.2; however, in some states, in the order in which they appear in Table 3-1, we identified specific legislation covering the private sector as a whole to which we have not yet referred.

CALIFORNIA

In California, lie detector tests are prohibited with respect to employment in the private sector (Cal Labor Code, sec 432.2). AIDS detection blood tests must be anonymous and the procedures for storing the results of such tests must not disclose the identity of the persons involved, even in response to a subpoena (Cal Health and Safety Code sec 199.20).

ILLINOIS

There are general privacy protection provisions in the Illinois Constitution: "The right of the people to be secure ... against the unreasonable interception of private communications by any means, shall not be violated" (Art 1, sec 6, Ill Constitution, 1970); and "Every person shall find a certain remedy in the laws for all injuries and wrongs which he receives to his person, privacy, property or reputation" (Art 1, sec 12, Ill Constitution, 1970).

It is illegal to alter a computer program to gain access to a system or to obtain the use or benefit of it without the owner's consent. Rights of civil action exist for victims of computer crime (Ill Rev Stat Ann ch 38, sec 16-9, as amended in 1983).

---

[41] **LAPERRIÈRE**, René and **PÉLADEAU**, Pierrôt, *Le droit sur la protection des renseignements personnels: Étude sur les bases privées de données à caractère personnel en droit canadien, comparé et international*. Montreal, 1986, SOQUIJ, 456 p.

The statute confers a right to obtain access and copies of personnel employment records, except letters of reference, management documents or security investigation records. No data concerning activities outside working hours may be collected (Ill Ann Stat ch 48, sec 2001).

CONNECTICUT

Here, we find again that there is scattered legislation covering the private sector, specifically covering computer crime (Conn Gen Stat Ann 53a-250) and employment records, the latter providing that private and public sector employees have the right to inspect their own records upon written request. The organization or firm must correct inaccuracies or include the correction made by the employee (Conn Gen Stat Ann 31-128a). An employer may not establish a blacklist of employees or use lie detectors or similar equipment (Conn Gen Stat Ann sec 31-51 and 31-51g).

TEXAS

In this state we find legislation concerning the confidentiality of medical records in the private sector (Tex Rev Civ Stat Ann Art 5561h, sec 13[d]) with, however, an exception for AIDS cases (Art 4419b-1, sec 9.01 [Ch 543, 1987 Sess]). There is also legislation respecting computer crime (Tex Penal Code Ann 33.01 and Tex Civ Stat Ann Art 5429b).

NEW JERSEY

Apart from the common law protection of privacy, the only general personal data protection legislation in the private sector in New Jersey is the recognition of civil and criminal liability for computer fraud (NJ Rev Stat Ann sec 2A:38A-1 and sec 2C:20-1).

3.2.3 *Other countries*

The relevant national legislation in most of the other countries to which Canada exports personal data excludes the private sector from its field of application. Nonetheless, we should note that in Australia the Privacy Commissioner must, pursuant to section 27(n), encourage the private sector to develop personal data management codes of conduct based on the OECD Guidelines.

We noted earlier that the Japanese legislation covers only automated files in the publi[illegible]r alone and contains no provision respecting transborder pe[illegible]al data flows. Italy and Singapore have no legislation designed to protect personal data in any sector whatsoever.

With respect to Hong Kong, we already know that a committee has been formed to draft personal data protection legislation. It seems that the legislation to be enacted by Hong Kong will cover only certain activities of the private sector and will, therefore, be rather sectoral in nature. Insurance and credit agencies, among others, have been designated as sectors to be covered by personal data protection legislation.

4 Analysis of results by public sector group

The purpose of this section is to comment on the results of our study dealing with the various groups of public sector organizations. In addition to analyzing certain cases that require mention because of the number of occurrences of transfers to the same country or the particularly large volumes of personal data involved, we will describe the rules that may apply to personal data held abroad about Canadian citizens and residents.

To ensure that these figures are truly significant, we will examine only those destinations that involve at least 5% of respondents in a single group where that proportion represents at least four occurrences. When working with groups that may be relatively small, it is standard practice to set criteria that tie a minimum percentage to a minimum number of occurrences. Thus, because of the low number of respondents in the municipalities and other municipal organizations group that transfer personal data abroad, we will not examine this group. We will also examine those cases where there are very large volumes.

4.1 Education

4.1.1 Results of the survey

In the education subsector, respondents reported sending personal data to several countries. Most often this involved sending school records when students wished to register in educational institutions abroad. Generally speaking, school records were transmitted only upon a request to do so by the student. Transfer of the personal data was thus a function of the contractual relationship between the student and his or her school. The destinations of these transfers were not surprising. They were the countries where Canadians most often choose to pursue higher education (as shown in Table 4-1), except perhaps for Japan.

Table 4-1
Significant data transfers

Country	**Occurrences**	**Occurrences/N of respondents (%)**
United States	45	14.90
United Kingdom	31	10.26
France	23	7.62
Fed Rep of Germany	22	7.28
Japan	16	5.30

4.1.2 *Legal protection*

It should be noted that each of these countries has legislation covering personal data protection, at least in the public sector, that applies to school records when data are transferred to public educational institutions.

In the United States, the Family Educational Rights and Privacy Act of 1975 provides that in order to receive federal funds, district schools and colleges must permit students over 18 years of age, or parents of students under 18, to have access to educational records. They must also limit any other outside access and establish procedures for disputing and correcting errors in records (20 USC 1232g).

The Department of Education is authorized to exchange data with credit bureaus for the purpose of collecting unpaid student loans (20 USC 1080.3). To ensure that federal loan insurance is repaid, the Secretary of Education must enter into cooperation agreements with credit bureaus for the exchange of information concerning student borrowers. No such information, however, may be disclosed by the Department of Education unless it has been verified and a reasonable time has been allowed for the debt in question to be paid. The information must not be used for collecting student loans when such collection attempts are not appropriate, fair and reasonable or involve harassment, intimidation or false representations (Education Amendments of 1980, 20 USC 1080).

4.2 *Health and social services*

We have already seen that transborder flows in the health and social services group occur primarily in the health subsector, essentially among hospitals. The greater mobility of the Canadian public and, particularly of segments of the population who are the largest consumers of health services, may explain the large number of personal data transfers in this sector. Only one case reported to us indicated the export of very large volumes of personal data to Florida. It involved a pediatric hospital that transmits certain information items taken from personal files it holds to a firm in the same group or conglomerate for the purpose of producing statistics.

Table 4-2
Significant transfers, health and social services

Country	Occurrences	Occurrences/N of respondents (%)
United States	77	17.62
United Kingdom	26	5.95

4.2.1 *Legal protection*

In the United States, there is an exception to the Privacy Act of 1974 relating to the disclosure of medical records (5 USC 552a(f)(3)). Organizations may adopt special procedures or regulations restricting or limiting the right of access. A majority of organizations have in fact done so, in most cases providing that such records are accessible only to the doctor designated by the patient. In addition, psychiatric medical centres and hospitals funded by the federal government must take all necessary measures to protect the rights of the patient (52 USC 2689(d)(2)).

In addition, the Department of Health and Human Services has been mandated to establish a national system for the exchange of data on adoptions, which must be coordinated with the states and regional systems to facilitate the placement of children in adoptive families (42 USC 5113(b)(3)).

Title IV of the Social Security Amendments of 1977 (PL 95-216) permits other federal services (42 USC 111 and 611) and state unemployment agencies to obtain access to records of earnings held by the social security administration. The Deficit Reduction Act further requests states to carry out computer comparisons to eliminate fraud and duplications in the use of state programs and benefits and to inform the individuals concerned of the results of such comparisons so that they may dispute them (42 USC 1320b-7[a] and [c]). Canadian citizens receiving American public benefits are all affected by these provisions.

There are some specific provisions relating to personal data in the field of health and social services in Florida, which our study found to be a major destination for data concerning Canadians. Is this a result of the annual migration of Canadians to the sun belt? Whatever the reason, social security numbers cannot be used in Florida to identify clients or to manage a bank's automatic funds transfer system (Fla Stat Ann sec 659.062). Lists of public assistance recipients are public information but cannot be used commercially (Fla Stat Ann sec 409.355(2)(a)).

In the health and social services sector, we should perhaps note with respect to the United Kingdom that the Council of Europe has adopted, among other recommendations about the protection of personal data, Recommendation No R(81)1 on the regulations applicable to automated and medical data banks (23 January 1981), Recommendation No R(83)10 on the protection of personal data used for scientific and statistical purposes (23 September 1983) and Recommendation No R(86)1 on the protection of personal data used for social security purposes (23 January 1986). Although these recommendations are not obligatory, they nonetheless clarify and refine the protection in this sector.

4.3 *Government*

4.3.1 *Results of the survey*

Of all the public sector groups, the government group was undoubtedly the most active in terms of transborder personal data transfers. This significance was not owing to the number of occurrences (41 for this group compared to the education and health and social services groups with 73 and 87 occurrences respectively) or to the proportion of respondents who report transferring personal data (23% for this group compared to 24% for education). Rather, it is the high volumes involved that drew our attention to this group. Several factors may explain these phenomena. First, the leadership role taken by the Canadian government with respect to social policies and various compensation programs has in recent decades resulted in the government making periodic payments to hundreds of thousands of Canadians. The payment of this money may involve a transfer of personal data abroad if such payments must, for one reason or another, be sent abroad. With the increasing mobility of the Canadian population, it is not surprising that such data transfers are growing.

Another phenomenon linked with Canadians' increased mobility is the substantially increased cooperation among police in North America in recent years. This cooperation extends not only to the suppression of crime (transferring the criminal record of an arrested individual to another country) but also to the verification of a simple driver's licence record. Very large volumes of personal data must therefore cross our borders though not to any single destination. These data are sent wherever Canadians are found, including the United States, the Caribbean and Western Europe, to mention a few examples. Table 4-3 lists the destinations that passed our significance test. The presence of Japan on the list may be surprising because, to our knowledge, there are few Canadians living in that country.

Table 4-3
Significant transfers by governments

Country	Occurrences	Occurrences/N of respondents (%)
United States	37	20.56
United Kingdom	24	13.33
France	20	11.11
Fed Rep of Germany	15	8.33
New York	13	7.22
Japan	10	5.56

4.3.2 Legal protection

We have already considered the situation in countries other than the United States. In addition to the general provisions that we discussed for the United States, we might note the following items at the federal level.

The Occupational Safety and Health Act (29 USC 657, 29 CFR 1910.20) permits the federal government to require employers to disclose certain medical data in employment records, records that employees are permitted to consult.

Federal government agencies may not sell or rent lists of addresses unless they are so authorized by law or required by the Freedom of Information Act (5 USC 552a(n)).

The Federal Election Campaign Act requires a candidate for federal office to report the name and address of any person who gives $50 or more, plus the occupation and principal place of business of anyone who contributes more than $100. This information is public but cannot be used by other fundraisers for other political organizations or for commercial purposes, except for the sale of periodicals (2 USC 438).

The Tax Reform Act of 1976 reverses the previous emphasis placed on the confidentiality of individuals' income tax returns. Although such returns are still confidential, there are exceptions. They may be disclosed with the consent of the taxpayer or his or her spouse to the administrator of an estate or to a member of a deceased's family; to a committee of Congress; to the Department of Justice or the Treasury for a tax investigation; to federal investigators for investigations not related to income tax (but with leave of a court); for statistical purposes; or to take action against parents who have not fulfilled an obligation to pay support. The President is authorized to consult the information contained in selected and designated individuals' tax returns, but only on the written request of the President himself and only if he reports to Congress every quarter with the names of the individuals. The President and the directors of agencies may also verify whether candidates for government positions are in good standing with the tax authorities (26 USC 6103).

All federal agencies are authorized to exchange information concerning recipients of loans or government guarantees and to disclose the identity of delinquent debtors to private firms. Agencies are permitted to access Internal Revenue Service records to trace a defaulting debtor and to demand the social security numbers of all loan applicants (Debt Collection Act of 1982, 28 USC 1 [note]).

Under the Law Enforcement Assistance Administration, the Department of Justice is responsible for the rules concerning security, confidentiality and privacy of data and criminal records held by the federal administration. These rules are published (28 Code Fed Reg 1).

Any individual is entitled to obtain a copy of information concerning him or her (42 USC 3771).

We might also note with respect to New York State that there are several statutes concerning privacy protection in the various government services. This legislation relates primarily to the confidentiality of tax records (NY Tax Law sec 697 [McKinney]), the confidentiality of library records (NY Civ Prac Law & Rules 4509) and the confidentiality of gas and electricity lists (NY Pub Serv Law, sec 65[7]).

5 Analysis of results by private sector group

The objective of this section is to comment on the results of our study with respect to the various groups of private sector organizations. As in the preceding section, we will deal only with those figures that are truly significant, using the test of four occurrences and 5% of respondents in the group in analyzing a specific destination. We will also examine those situations where very large volumes of personal data have been exported (concerning more than 10,000 individuals) during the last year or last five years, and those situations where personal data transferred abroad by the respondent concern a total of more than 100,000 people.

As we have seen, the results of our survey in the private sector were grouped into nine fields of activity: associations, insurance, industry and business, communications, financial services, transportation and tourism, computer services, professional services and miscellaneous services.

There is no specific protection covering these sectors of activity in Australia and Japan. We would note that these countries protect only nominative data relating to the public sector. In the case of Great Britain, France and the Federal Republic of Germany, the same approach noted earlier applies. Their legislation is general or universal in nature and governs *all* matters relating to the protection of personal data in the public and private sectors. It has a single and all-encompassing purpose. Thus, we do not find particular or specific provisions covering one or another of these nine fields of activity in these countries.

As we have already explained, in those jurisdictions that offer general protection or protection that is specific to the public or private sector, we have not researched specific provisions for each of the sectors considered in our study. We shall, therefore, consider such provisions only by exception in this part.

Thus, each time our study shows that for a particular sector there are large volumes of flows to a specific country, we will refer the reader to the comments we made earlier with respect to either general protection or protection specific to the public or private sector before considering the provisions that are unique and specific to the single sector in question. As a result, the following discussion is very succinct with respect to Europe. However, we will have to detail the protections offered in the various American states that do not have general protection but, rather, offer only sectoral protection.

Nonetheless, we would note that the British legislation contains specific provisions respecting "computer bureaus"[42]. Sections 4 to 8 of the British Act contain specific provisions concerning the registration of computer bureaus and access to personal data therein.

5.1 *Associations*

5.1.1 *Results of the survey*

The associations group covers a host of organizations such as professional bodies, various types of religious institutions, unions, private clubs and so on. With 36% of respondents reporting transferring personal data abroad, this group is one of the most open to the outside world. Religious institutions often employ and send employees abroad, personnel management normally involving transborder movements of personal data. Because of the increasing mobility of their members, professional bodies also have to transfer data about their members to various countries. Unions and, particularly, those affiliated with international unions, may transfer personal data about their members, one respondent reporting the transfer of personal data about all their members to a private firm in Washington State (personal data about 20,000 members during the last five years) for reasons that we could not determine.

Table 5-1 indicates the most important destinations of personal data transfers abroad. There are few big surprises. The countries on this list are those with which Canada has close relations. We might be surprised to see Singapore on this list. We note the role of this small country: it often serves as a bridgehead for the activities of several associations in this region of Asia.

---

[42] This expression is defined in an explanatory guide to the British Act as follows: "A person runs a computer bureau if either of the following conditions is met: a) he processes data for other people as their agent; b) he allows other people to process their data on his equipment. A data user can therefore be a computer bureau", Peat, Marwick. *The Data Protection Handbook*, London, Peat, Marwick, Mitchell & Co, 1984, pp 8-9.

Table 5-1
Significant transfers by associations

Country	Occurrences	Occurrences/N of respondents (%)
United States	19	25.68
Japan	8	8.11
United Kingdom	5	6.76
France	5	6.76
New York	5	6.76
California	5	6.76
Fed Rep of Germany	4	5.41
Washington	4	5.41
Singapore	4	5.41

5.1.2 *Legal protection*

In this group of the private sector, we did not identify any specific legislation in addition to the general legislation or legislation specific to the private sector as a whole that would cover personal data concerning Canadians in the states or countries of destination.

The associations sector is extremely varied and is often the subject of general or specific legislation in that the right of association is considered everywhere to be a fundamental freedom essential to the exercise of democratic rights. This sector covers political parties as well as religious communities. There are numerous provisions in these areas that are not grounded in a concern for personal data protection but which have that incidental effect. In addition, several types of activities of associations are governed by quasi-contractual measures such as association by-laws or membership contracts. We refer here to the discussion in section 8 of the preceding chapter with respect to our analysis of responses to the questions on the nature of the data transferred, primarily with respect to memberships and affiliations.

5.2 *Insurance*

5.2.1 *Results of the survey*

If we had to identify the subsectors that reported transferring the most personal data abroad, we would have to nominate the insurance group. Not only is it the one that transfers the most personal data (with a rate of 35% of respondents exporting data), but the volumes transferred abroad are also impressive. Table 5-2 shows that the United States was the preferred destination for transborder personal data flows in this group; 26.51% of respondents reported transferring data there. However, 88% of all those that transferred personal data abroad sent it to the United States. While life insurers particularly contribute to this flow to the United States (because of the personal data about each of their clients transferred to the Medical Information Bureau in Boston, Massachusetts), they are probably not the only insurers that transfer personal data to the United States. Although Massachusetts is the destination reported most frequently, other American states also receive large volumes of personal data from Canada.

Table 5-2
Significant transfers, insurance

Country	Occurrences	Occurrences/N of respondents (%)
United States	22	26.51
Massachusetts	5	8.43

Table 5-3 shows the insurers that transferred very large volumes of personal data. Here we found 11 respondents in the insurance group (all in the "insurers" subsector) who exported very large volumes of personal data. Three of the five respondents in this group who transferred personal data to Massachusetts exported large volumes. However, eight other insurers send personal data elsewhere in the United States.

The Canadian and British Insurance Companies Act (RSC 1985, c I-12) and the Foreign Insurance Companies Act (RSC 1985, c I-13) do not require an insurer to retain a copy of records of transactions involving clients in Canada, as does the Bank Act (ss 157-159, RSC 1985, c B-1). Thus, it is probable that subsidiaries of American insurers transfer all their personal data to their head office in the United States for processing.

Table 5-3
Destinations of high volumes, insurance group

State	Subsector	Last year (10,000 +)	Last 5 years (10,000 +)	Total (100,000 +)
Massachusetts	insurance	75,000	375,000	
	insurance		10,000	
	insurance	92,000	460,000	
Florida	insurance		20,000	
Washington	insurance	200,000		200,000
Pennsylvania	insurance		12,000	
Illinois	insurance	40,000		
New York	insurance	150,000	600,000	150,000
State not specified	insurance	10,000	50,000	
31-50 states	insurance	10,000	55,000	
State not specified	insurance		40,000	

5.2.2 *Legal protection*[43]

1. In the United States there are various statutes specifically concerning the protection of personal data in the insurance sector. At the federal level, there is no specific legislation on insurance. However, insurance companies that use consumer or credit reporting agencies must comply with the provisions of the Fair Credit Reporting Act (15 USC 1681), which permits consumers to learn the nature, content and sources of the information (except medical information) collected and held by a consumer reporting agency. In the event of disagreement, the consumer may demand that his or her version of the facts also be placed in the record.

2. In addition to the general legislation already discussed, it is worth noting that Massachusetts law sets limits to the contents of credit reports. For instance, no arrest that occurred more than seven years ago, nor any bankruptcy older than 14 years, can be reported (Mass. Gen. Laws Ann. ch. 93, sec. 52). The consumer must be informed when an investigation takes place (sec. 53) and has the right to ask for the results and to challenge them (sec. 59). It is not clear, however, whether strangers can resort to the mechanisms provided by the law.

   Because such large volumes of personal data are sent to this state, we would note that this is the location of the Medical Information Bureau, which handles the processing of medical files on various insurance policy applications for a large consortium of insurers. In these circumstances, it is useful to note the medical data protection legislation known in Massachusetts as the charter of patients' rights (Mass Gen Laws Ann ch 111, sec 70E; also ch 123, sec 36 and ch 149, sec 19A). Because this legislation sets out the rules that insurance companies must follow, it would protect data concerning Canadians indirectly; however, it is not clear whether Canadians may directly exercise the remedies and rights of access and correction provided therein.

---

[43] In relation to insurance, we would refer the reader to the GRID study: *Le droit sur la protection des renseignements personnels; Étude sur les bases privées de connées à caractère personnel en droit canadien, comparé et international.* Montreal, 1986, SOQUIJ, 456 p, at pp 303 to 329.

3. We did not identify any specific provision or legislation in the insurance sector in New York State, except for the fact that it is illegal for an employer, an insurance company or a credit bureau to inquire into an arrest of an individual that did not lead to a conviction (NY Exec Law 296.16). Nor did we find any specific legislation concerning personal data protection in the insurance field in either Florida or Washington State.

4. The Illinois Privacy Law (Ill Ann Stat ch 73, sec 1065.701 to 724) is based on the Insurance Information and Privacy Protection Model Act: 1979, developed by the National Association of State Insurance Commissioners[44]. Companies must provide their clients with a notice setting out the types and sources of information held by the company and informing them of the right of access and correction. The client may ask to be informed of the reasons for refusal to insure. The authorization forms used by insurance companies to obtain personal data must be dated and written in simple language and must specify to whom the information may be disclosed. The form must have an expiry date. AIDS tests may not be administered without the consent of the patient and results must be anonymous. Results may not be disclosed outside the health services community without the consent of the patient or a court order. Insurers may, with the consent of the patient, require such a test and must keep the results confidential (Ill Ann Stat ch 1111 1/2, sec 7301. PA 85-677).

5. There is no specific legislation on insurance records in Pennsylvania, except the statement of principle in the Constitution (Pa Constitution, Art 1, sec 1) recognizing the right of "acquiring, possessing and protecting property and reputation" as one of the "inherent rights of mankind". This statement has been broadly interpreted with respect to personal data.

---

[44] We might note here that the California *Insurance Information and Privacy Protection Act* (Cal Insurance Code: Art 6.6, sec 791 et seq; the Connecticut *Insurance Information and Privacy Protection Act* (Conn Gen Stat Ann Sec 38-500) and the Virginia *Insurance Information and Privacy Protection Act* (Code of Va, sec 38.1-57.2 et seq) are almost identical and implement the uniform Bill.

5.3 *Business and industry*

5.3.1 *Results of the survey*

There was great diversity in the business and industry group where 27% of respondents reported transferring personal data. We noted initially that manufacturing industry (36%) and primary industry (43%) were mainly responsible for the transfer of personal data abroad. We then saw that a majority of the subjects of the personal data disclosed were employees (97%), data concerning clients (16.1%) and other individuals (6.5%) rarely being transferred abroad. Finally, we found that 71% of respondents in this group transferred personal data to another part of the same multinational.

The profile of this group shows firms that export personal data about their employees so it can be processed by their company's head office. Thus, it is not surprising to find that the United States was the primary destination, as shown in table 5-4. We should also note that 31 respondents in this group reported transferring personal data abroad and, of these, 30 or almost 97% transferred the data to the United States. It is not, therefore, difficult to conclude that we were dealing largely with American multinationals. Given that the United Kingdom is often the base for the European operations of American firms, it is not surprising to find the United Kingdom as the other country to which personal data were transferred. It should be noted that one respondent in this group transmitted very large volumes of nominative data; this type of data, relating to 150,000 clients, is held in California. However, this firm is in the retail/wholesale business subsector.

Table 5-4
Significant transfers, business and industry

Country	Occurrences	Occurrences/N of respondents (%)
United States	30	27.27
United Kingdom	15	13.64

5.3.2 *Legal protection*

In addition to the general provisions of the British legislation, which we have already examined, we should perhaps note that the Council of Europe has adopted, among other recommendations concerning personal data protection, Recommendation No R(85)20 on the protection of personal data used for direct marketing purposes (25 October 1985). Although they are not obligatory, these recommendations nonetheless clarify and refine the protection in this sector. We did not identify specific legislation in this sector beyond the American federal legislation and the California legislation already noted.

5.4 *Communications*

5.4.1 *Results of the survey*

As we have seen, the communications group exports very few personal data abroad. Only 13% of respondents reported transferring this type of information (10 out of 77 respondents in this group). Surprisingly, these personal data related mainly to employees (70% of exporters) while clients (with 20%) and other persons (20%) were scarcely affected. This may be explained by the fact that in half the cases the data were sent to another part of the same multinational.

Given these circumstances, it is not surprising to observe, as shown in Table 5-5, that the United States is the only destination to which significant flows were sent. We should also add that one firm in this group, a cable TV firm, reported transferring personal data to California for billing purposes. This operation involved transferring personal data on about 20,000 clients during the last year, but the cable firm reported that clients' personal records are not stored in California.

Table 5-5
Significant transfers, communications group

Country	Occurrences	Occurrences/N of respondents (%)
United States	7	9.09

5.4.2 *Legal protection*

1. The governing principle in the field of communications in the United States is "To safeguard the privacy of innocent persons, the interception of wire or vocal communications where none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court" (18 USC 2510).

   There are few exceptions to this rule: telephone companies, the Federal Communications Commission, police officers who are parties to a conversation and communications where one party consents fall within such exceptions. There is also specific legislation covering espionage (50 USC 1801). Federal legislation now covers cellular telephones, electronic mail and data transfers, it being an offence to intercept them[45]. The Electronic Communications Privacy Act of 1986 (18 USC 121 ss 2701 et seq) also makes it an offence to use electronic data recording or communication services without authorization, to intercept a communication or to disclose the contents of a communication in an electronic bank or mail service.

---

[45] *Electronic Communications Privacy Act* of 1986, PL 99-508, amending 18 USC 2511, 3117, 2701, 3121, *inter alia.*

There is also legislation concerning the protection of personal data in the cable TV industry. The Cable Communications Policy Act of 1984 (47 USC 551) gives a subscriber the right to be informed, to control, to have access to and to correct his or her personal data. It imposes standards on the cable firm respecting the storage and transfer of the data it holds.

2. We did not identify any specific legislation in the communications sector in California, except the provision prohibiting telephone solicitation using an automatic recording system (Public Utilities Code sec 2821-25) and the fact that it is an offence to intercept a telephone or telegraph message and/or to disclose its contents (Cal Penal Code sec 631 through 637). This ban even includes cellular telephones (sec 632.5), and telecommunications companies must take "adequate steps to insure privacy of communications over (their) systems" (Cal Pub Util Code sec 7905).

   There is also a statute concerning the protection of personal data in the cable TV industry (Cal Penal Code; sec 16-633) that imposes a duty of confidentiality on cable firms and prohibits them from transferring personal data to public organizations without a court order.[46]

5.5 *Financial services*

5.5.1 *Results of the survey*

The scattered cases in the financial services group make it very difficult to draw general conclusions. It will, however, be remembered that personal data transfers abroad related largely to clients (70%), data transfers concerning employees (23.5%) and other persons (12%) being much less common. Of course, the United States was the primary destination for personal data transfers (see table 5-6).

Table 5-6
Significant transfers, financial services

Country	Occurrences	Occurrences/N of respondents (%)
United States	13	16.05

It must be noted, however, that some firms in this group transferred very large volumes of personal data abroad. Two firms transferred such data to more than 20 countries. We note that one credit bureau, the only bureau that decided to respond to our questionnaire, transferred very large volumes of personal data only about people who were neither employees nor clients.

---

[46] See GRID study, op. cit., pp 365 to 387.

Table 5-7
Destination of large volumes, financial services

Destination	Subsector	1 year (10,000 +)	5 years (10,000 +)
Multiple (more than 20 countries)	credit bureau		15,000
	financial services	10,000	50,000

5.5.2 *Legal protection*

Given that our study has shown that the United States in general is the main destination for personal data flows concerning Canadians, we will examine here only the federal legislation, referring to earlier GRID studies for an analysis of state legislation.

Despite the fact that the confidentiality of financial and banking data is, in a way, the cornerstone of this industry's credibility and so it should not be necessary to enact specific legislation to ensure confidentiality, nonetheless there are numerous pieces of American legislation protecting personal data in the financial and banking field.

Under the Right to Financial Privacy Act of 1978, almost all federal investigators must present a request in writing or as otherwise provided by law to have access to an individual's financial records in a financial institution, including credit card companies. A federal agent must simultaneously give notice to the individual, who may object to such access being given. A 1979 amendment relieves financial institutions of the responsibility of informing clients that such protection exists (12 USC 3401). The Tax Reform Act of 1976 (26 USC 7609) contains a similar provision.

The Electronic Fund Transfer Act, in effect since May 1980, provides that institutions that offer electronic banking services must inform clients of the circumstances in which data on their accounts may automatically be disclosed to a third party in the ordinary course of business (15 USC 1693 c(a)(9); also 12 CFR 205.10). Consumers have the right to know the nature, content and sources (except sources of inquiries) of information (except medical information) held by investigation and credit agencies. Companies must purge their records of obsolete data and must reinvestigate when there is a dispute. If the disagreement is not resolved, the consumer may enter his or her version of the facts in subsequent reports.

The Fair Credit Reporting Act (15 USC 1681-1681t) governs corporations that investigate and examine client records in the areas of credit, insurance or employment. Its objective is to ensure that these activities result in fair records, that the personal data therein are correct, complete, relevant to the intended use and stored in a manner that respects confidentiality.

The peculiarity of this federal legislation is that it applies to all agencies that use means or facilities of interstate commerce in preparing or furnishing credit reports (sec 1681(f)).[47]

There is also other legislation in this field designed to protect privacy: for example, the Equal Credit Opportunity Act (15 USC 1691), the Fair Credit Billing Act (15 USC 1666) and the Fair Debt Collection Practices Act (15 USC 1692). Because these statutes impose duties and prescribe procedures to be followed by the holders of data themselves, we may say that they indirectly protect Canadians.

5.6 Transportation and tourism

5.6.1 Results of the survey

The transportation and tourism group ranked last among personal data exporters, being the group in which the lowest proportion of respondents reported transferring personal data abroad. Contrary to what we might assume, these transfers more frequently related to employees (70%) than to clients (60%), a majority of transfers involving transactions between two parts of the same multinational (60%). Table 5-8 shows that the preferred destination for personal data transfers, as it is for Canadian tourists, is our American neighbour.

Table 5-8
Significant transfers, transportation and tourism

Country	Occurrences	Occurrences/N of respondents (%)
United States	8	6.06

When firms in this group transferred personal data, however, there may have been high volumes involved. As Table 5-9 shows, four of the 10 respondents who reported transferring personal data sent data concerning at least 10,000 individuals during the last five years. Although these were employees in the case of a transportation company, in all other cases the people concerned were clients. One could say therefore that while few firms transferred personal data, those that did so reported transferring a lot. In Table 5-9, the destination of the "multiple" occurrence was the United Kingdom, the United States and other American countries. The letter (e) indicates employees.

---

[47] "Which use any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports."

Table 5-9
Destination of large volumes, transportation and tourism

Destination	Subsector	1 year (10,000 +)	5 years (10,000 +)	total (100,000 +)
Florida	tourism	51,000	185,000	
Missouri	tourism	102,000	150,000	150,000
Connecticut	transport		10,000 (e)	
Multiple	tourism	100,000		

5.6.2 *Legal protection*

We did not identify any specific legislation here concerning the protection of personal data in the field of transportation and tourism in the United States or in the states that are the destination for large volumes of personal data, such as Florida, Connecticut or Missouri.

5.7 *Computer services*

5.7.1 *Results of the survey*

The computer services group has one of the highest proportions of respondents transferring personal data (36%). This is not unusual in that this industry exists by collecting, processing and transmitting information. Nor can we be surprised that such transfers may relate to individuals.

However, we may wonder about the fact that more respondents in this group transferred data about their employees (75%) than about their clients (50%) or other persons (17%). Perhaps they confused data relating to their clients' employees, which might be transferred abroad, and data about their own employees. In any event, the primary destination for transborder personal data flows was the United States. Data transferred by 11 of 12 respondents who reported transferring personal data abroad were sent to that country.

Table 5-10
Significant transfers, computer services

Country	Occurrences	Occurrences/N of respondents (%)
United States	11	33.3

5.7.2 *Legal protection*

For the United States, we identified only the legislation discussed earlier relating to computer crime or wiretapping that might protect personal data in the computer services sector. Because we described it in full above, we note here only that the Electronic Communications Privacy Act of 1986 (18 USC 121 sec 2701 et seq) also makes it an offence to use, without authorization, electronic data recording or communication services, to intercept or disclose the content of a direct communication or a communication recorded in a bank or electronic mail services.

5.8 *Professional services*

5.8.1 *Results of the survey*

According to the response to our survey, the professional services group was the most internationalized of all the groups. In all, 38% of respondents report transferring personal data abroad with a high of 44% in the accounting profession alone. This group is distinguished by the fact that it transferred personal data not only to the United States (the 14 respondents who report transferring personal data all send data to the United States and, particularly, to New York State and Florida) but also to the United Kingdom, France, Japan, the Federal Republic of Germany and as far away as Australia.

Table 5-11
Significant transfers, professional services

Country	Occurrences	Occurrences/N of respondents (%)
United States	14	37.84
New York	10	27.03
United Kingdom	9	24.32
Florida	8	21.62
France	7	18.92
Japan	5	13.51
Fed Rep of Germany	4	10.81
Australia	4	10.18

5.8.2 *Legal protection*

This is a bit of a catch-all category that is not addressed specifically in legislation, and it would be difficult to restate the comments we have made already for each country of destination of personal data flows in the miscellaneous professional services field.

1. We did not find any specific legislation protecting personal data in the United States as a whole, apart from the provisions concerning what is referred to as privileged communications between professionals and their clients: lawyers, doctors, pastors, psychologists and so on. Protection of these particular personal data is based on

an interpersonal relationship and is governed primarily by the common law of the country.

2. Given the importance of these flows, we should perhaps note that in New York State, communications with doctors and nursing staff are recognized as privileged (NY Civ Prac Law sec 4504 (McKinney)) and that patients have a right of access to medical records concerning them under established rules (Rules of the New York State Board of Regents Relating to Definitions of Unprofessional Conduct [1977] 29.2[a][7]; 29.1[b][13]). This state also recognizes that communications with dentists are privileged and confidential (NY Civ Prac Law sec 4504) as are communications with members of the clergy (sec 4505), psychologists (sec 4507) and social workers (sec 4508).

3. Florida also recognizes that communications with both doctors and psychiatrists are privileged (Fla Stat Ann sec 90.542). For medical records, a licensed health care provider must give to a patient, or a patient's legal representative, copies of his or her records upon request (Fla Stat Ann sec 395.202) and may not disclose such records to anyone else without the consent of the patient except when so compelled by subpoena (Fla Stat Ann sec 455.241 and 395.017, amended in 1983).

5.9 *Miscellaneous services*

5.9.1 *Results of the survey*

The miscellaneous services group deals with situations that are so diverse that it is difficult to draw any general conclusion at all. Despite this diversity, as Table 5-12 shows, there is one destination that appears very frequently for personal data concerning Canadians: the United States. France, as we know, holds a leading position in the field of services exports. Because 80% of personal data transfers in the miscellaneous services subsector occur within the same multinational, it is not surprising to find the two leading exporters of services in the world on this list.

Table 5-12: Significant transfers, miscellaneous services

Country	Occurrences	Occurrences/N of respondents (%)
United States	9	22.50
New York	7	17.50
France	4	10.00

It should also be noted that the only marketing firm that reported engaging in personal data transfers abroad informed us that it transferred data about more than 500,000 people (who were neither clients nor employees) during the last year to New York State and Illinois.

5.9.2 *Legal protection*

1. Despite the fact that the activities grouped under this heading are very general and disparate, the legislation discussed earlier is supplemented by several pieces of specific legislation that may influence the protection of personal data in the United States. People and firms regularly preparing other people's income tax returns may not disclose personal information or use it for other purposes, with certain exceptions set out in the Internal Revenue Service Regulations (42 USC 7216).
2. In New York State, retail stores that provide information to credit reporting companies must notify the individual in writing, stating the name of the company. The insertion of false information in an individual's credit report is punishable by a fine or one year in prison if such an act causes damage or prejudices the individual (Gen Bus Law sec 380 and sec 387). New York State credit services legislation is similar to the California legislation to which we referred earlier (Gen Bus Law sec 458a).

   Gas, electricity and water services may not sell lists of their clients (NY Pub Service Law sec 65[7]) nor may telegraph and telephone companies sell lists of people whose names and numbers are not published in the telephone directory (NY Pub Service Law sec 91). No credit card registration service may rent, sell, exchange or otherwise make available the names, addresses and credit card or other financial institution account numbers to a third party for mail advertising or solicitation without the prior written agreement of the cardholder (NY Gen Bus Law sec 521-c).
3. In addition to the general provisions in the French legislation examined earlier, we might note that the Council of Europe has adopted, among other recommendations concerning personal data protection, Recommendation No R(83)20 on the protection of personal data used for scientific research and statistical purposes (23 September 1983) and Recommendation No R(85)20 on the protection of personal data used for direct marketing purposes (25 October 1985). Although these Recommendations are not obligatory, they nonetheless clarify and refine the protection offered in this sector.

5.10 *Residual contextual law*

It may be well to note that the sectoral analysis that we have just set out may have left out some provisions of a general nature that were described as "contextual law" in the analysis in *L'Identité Piratée*. It should be noted that we did not have a mandate to study all legislative and judicial systems covering all transferees of personal data flows but, rather, only those provisions that seemed most directly related to the protection of personal data concerning Canadians in the jurisdictions of destination.

6 Summary and conclusions

If we consider all the information yielded by our survey with respect to the countries of destination for personal data transfers from Canada, it is impossible to draw monolithic conclusions.

Clearly, the primary destination of transborder personal data flows is our primary trading partner, the United States of America. Of course, apart from the United States, all regions of the world receive personal data sent from Canada. But this is where our generalizations must stop.

The public sector appears to have much more diverse destinations than the private sector, with a particular predilection for the European countries. Few large volumes of personal data are exported by this sector, except by the government group in which several respondents report transferring large amounts of personal data to more than 20 countries.

In the private sector, the attraction of the United States seems to be irresistible. The economic integration of the North American subcontinent results in a significant transfer of personal data, sometimes characterized by transfers of very large volumes of personal data to another part of the same multinational based in the United States (for example, insurers). It should be noted that ties with the Pacific region countries result in a larger number of personal data transfers by the private sector than by the public sector, unlike the situation with respect to the European countries.

In the area of the legal protection that has been implemented by the various countries in order to protect personal data, only those countries that are parties to the European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data seem to guarantee general protection for personal data transferred from Canada. Other countries grant protection only to personal data held by public organizations, while some offer no protection. In the United States, the general protection afforded to personal data held by the public sector is supplemented by a long list of sectoral protective measures that, most often, vary from state to state.

SUMMARY AND GENERAL CONCLUSIONS

1 Originality and limits of the study

1.1 Characteristics of the objective of the study

This study was intended essentially to describe and assess the situation with respect to the export of personal data concerning persons living in Canada, including the origin, destination, volume and nature of these data. It was also intended to identify the legal protection enjoyed by such data once they reached their destination abroad. Within an overall review of the Privacy Act, this study fulfills a part of the Government of Canada's commitment to respond to concerns expressed by members of Parliament about transborder flows of personal data.

This particular context, as well as the strict time constraints imposed, defined the approach taken and the limits of the study. Given that the central concern was the protection of Canadians' privacy and the primary subject matter was personal data, we attempted to identify where exports of data concerning Canadians occurred and to determine the major characteristics of such exports from the point of view of protecting individuals' rights. We did not, therefore, attempt to analyze the other contextual variables (i.e., technological, economic or political factors), except where they might have a direct influence on the major issue in our study. Our study is, therefore, distinct from the main current in the literature and empirical studies of the issue of transborder data flows, which have been until now considered primarily from the commercial and technical angle (free flow of information, communications networks and so on).

In addition, our study was designed to collect facts about the identity of the parties involved (exporters and recipients), the volumes of data flows, the nature of the data exported, the destination of the flows, the methods by which data are disclosed and the legal protection to which data are subject. Unlike most other comparable studies, our goal was not to determine the opinion of our participants on the issue but, rather, to invite them to construct an image of the situation as it existed in Canada in the fall of 1989.

We had to take into account two important characteristics of our topic of study: it is new and it is complex. We did not restrict ourselves to computerized data transfers. Clearly, however, the rise in the level of concern about the protection of the rights and freedoms of the people on whom data are held and the enactment of legislation to protect rights in this field have been prompted by the burgeoning of new information technologies. Computers and telematics are rapidly evolving and expanding, requiring that practices be quickly adapted to new developments. It should not be surprising that these products have not been analyzed, let alone conceptualized, not only by researchers but also by the users of these technologies. Data subjects are often totally unaware of what is being done with data that have been collected on them, often with their consent. The state of our understanding of the issue is thus embryonic, as it is for a large number of organizations. As a result, this study is essentially exploratory.

However, we should not underestimate the expertise that has been developed on this issue within very large organizations on the cutting edge of technological developments. They cannot afford to ignore or fail to master the fundamentals of the management of their important personnel files, either because of the competition they face (in the private sector) or the legislation they must apply (in the public sector). In this respect, we found notable differences in the quality of the responses sent to us, reflecting a wide range in the levels of understanding of the issues under examination.

One of the important aspects and concerns of our study was the analysis of the foreign legal protection enjoyed by personal data exported from Canada concerning Canadians. Apart from foreign legislative sources and the organizations that we consulted in various countries, we asked our respondents a number of questions about the main protections and guarantees provided at the time they effected transborder flows. To deal with the concern for data protection, the questions asked in our survey all related to this issue. The protection question is part of a larger issue that is, in part, legal because the primary methods of protection now in effect are legal in nature. Similarly, questions about transferees, purposes, the nature of the data and methods of transfer resulted from our concern that we find the best means of protecting personal data.

Research into the protection that exists abroad for Canadian data was relevant to this concern in two respects: we wished to assess both the effects of these exports on the rights of Canadians and to assess the protection requirements that may exist in certain foreign countries in relation to data exported to Canada from their territory — data that are protected by statutes, regulations, constitutions and conventions at home. The concern about personal data protection is an entirely original element in this study. It has had an impact on the research objective and the methodology and makes this study particularly useful in assessing any action that might be taken to ensure greater control over this phenomenon.

1.2 *Characteristics of the subjects of the study*

One of the major characteristics of our study is that, although we limited our work to an analysis of the situation in one country, Canada, the study covers all economic and administrative sectors operating in all regions of the country. The size of the population studied (5,291 questionnaires) makes it a major study. The rate of response obtained (36.3%) was quite exceptional. Rather than establish a representative sample of this population, a task that would have been difficult given the limited state of knowledge on this subject, we targeted the largest firms and organizations in Canada and those most likely to be involved in international personal data flows. The results of our survey allowed us to establish that the size of the firm or organization was a variable that had a determinative effect on whether such flows occur. We might assume that this is also true for smaller firms and organizations, which we excluded from our study.

As the state of knowledge of the phenomenon we were considering was very deficient, we had to look to the only parties who might have some structured knowledge in this area, the data exporters themselves. This meant that this study did not include lobby groups and the people who are the subjects of flows of data being exchanged. This is not to say that their participation would not have been useful; rather, we believed that their contribution would have been more difficult to obtain and to use, given the little information that they actually have on this topic and given that we were attempting to establish the facts and measure the scope of the phenomenon. Their contribution will undoubtedly be essential when, in light of the results of our study, we come to assess the best means of controlling the phenomenon and illustrate the problems and issues involved using specific cases.

If we compare the results of our study with those of other studies, ours contains a considerable quantity of factual data on the situation of transborder personal data flows, while other comparable studies at most provided little information about the existence of such flows. For these other studies, the main objective was to study the media of transfer and to solicit opinions from respondents. However, the facts collected through our survey came from the voluntary reporting of our respondents and their assessments of the situation within their organizations. To the extent that the respondents were able to provide specific facts, we have no reason to doubt they provided us with a reliable description of the situation.

However, it became clear that the specific approach we took was very demanding on our respondents. To encourage them to provide us with the most information possible, we guaranteed absolute confidentiality. A majority of our respondents took up this offer and did not identify themselves on the questionnaire. It was, therefore, impossible for us to analyze the origins of the responses in a detailed manner, apart from determining the respondent's economic or administrative sector. Given the growth in competition in the information markets and the application of legislation in the public sector, our respondents had to be discreet. In our view, preservation of confidentiality was a necessary condition for obtaining a critical mass of relevant information.

We also found ourselves at the intersection of several scientific approaches to the phenomenon under study and in an area of great complexity: communications. Our survey could not require our respondents to do an extensive internal investigation of their firm or organization to determine the necessary facts as precisely as possible. Some organizations and firms obviously took great care in assembling the figures and they must be congratulated. However, there is not always a personal data transfer expert within an organization who can quickly bring together the available information and organize it in relation to our survey's main concern, the protection of personal data. In fact, our survey became well-traveled, moving from one branch or division to another, some of the delays in responding clearly being attributable to the difficulty in gathering the facts to respond as accurately as possible.

In addition, not wanting the effort to appear too difficult for some respondents, we suggested that they give us approximations if this was the best available information or indicate that their volumes or percentages were impossible to estimate. A majority of respondents took this opportunity, which was unfortunate in a way, but which resulted in more responses and more realistic responses. This gave us a better idea of what lay ahead and the effort that would be required to complete our description of the situation.

We observed that participation in our study was very low in some sectors of activity, and that some sectors provided figures that did not always correspond with what we knew from our experience or with the experience of any individual who is concerned with his or her rights and has traveled or done business abroad. The low rate of participation in some groups, or the approximated responses provided by some respondents under cover of anonymity, may substantially distort the picture of the situation that emerges from our study. This may make it necessary to subject the practices of these groups to more constrained methods of investigation. Some of the figures from our survey seemed to us to be clearly incomplete or incongruous. We noted these in our analysis, particularly for the finance and air transportation sectors. On the basis of these figures we would recommend that further studies be conducted using finer tools and methodology, in order to better grasp the situation in some sectors where the picture presented to us seems to be inadequate.

1.3 *Characteristics of the method used in investigating and reporting*

We are also aware that conducting a postal survey presents a number of disadvantages in comparison with other qualitative methods such as semi-directed interviews, which permit a more thorough analysis of significant cases. For example, one of the major disadvantages of our survey is that we could not cross-tabulate multiple questions in an area where everything is very interrelated and where assessing the situation depends on assessing multiple variables operating at the same time.

However, given the short period of time we had to conduct this study (less than six months), and given the objectives, it was impossible to go into more detail. What we gained in quantity we likely lost in quality of information.

Nonetheless, our survey did enable us to bring together a remarkable quantity of data about international personal data flows from Canada, not only by broad sectors of activity (public and private) but also for 13 groups of activities (four in the public sector and nine in the private sector) and for 48 distinct subsectors. These were studied with respect to the existence of transborder flows, the size of the organizations and the jurisdictions under which they operate. This information suggests an overall assessment in each of these sectors or subsectors. Eventually, it will be possible to do a more thorough analysis using other approaches when the situation in a sector justifies such research or the information provided appears to be inadequate.

Our method of describing the results enabled us to provide a question-by-question report, setting out the characteristics of each sector and comparing sectors for each of these characteristics. After summarizing these results in point 2, we will provide a further summary in point 3, this time based on the groups of sectors and highlighting the results we found from our study for each sector. This breakdown will permit us to do a general comparison and to better highlight the significant points because, not only will it bring out the substance of our respondents' reports: it will also show where they are inadequate or nonexistent. In point 4, we will assess these results to propose overall conclusions and to determine the general significance of the study, concluding with an assessment of this research experience.

2 Summary of conclusions from the questions examined

2.1 *Characteristics of exporters*

Our survey revealed that in Canada as a whole 21% of the largest public organizations and private firms engage in international exchanges of personal information relating to Canadians. A slightly higher proportion (24%) of the private sector firms (one third indicating they operated under federal jurisdiction) than public organizations (20%) exported such data. While there was relative uniformity among public organizations (with the exception of municipalities, which exported very little), the rates varied considerably for private firms depending on the field of activity. In the sectors where we would have anticipated large flows, relatively few were stated to occur (transportation and tourism, 8%; communications, 13%). Others were about average (finance, 21%; miscellaneous services, 25%; business and industry, 27%). Greater activity was reported in the fields of insurance (30%), associations (35%), computer services (36%) and professional services (38%).

By examining the results by subsector, we were able to draw even finer distinctions in our results by identifying the groups of firms that export large amounts of personal data: personnel employment agencies, travel agencies, primary and manufacturing industries, publishers, banks, real estate agents, advertising agencies, and federal departments and organizations. On the other hand, very few transborder personal data flows were reported in some other subsectors: transporters (including air transporters), electronic and telephone communications firms, credit institutions, investment companies, credit bureaus, securities brokers and security services.

We observed that the size of the firms and organizations was a major factor in determining the existence of transborder personal data flows. In general, the larger a private firm in terms of employees, the greater the chances that it engaged in such flows. The larger a public institution in terms of number of clients (or persons under its administration), the greater the chance it did the same. Moreover, relatively few private firms or public organizations (7%) used intermediaries to effect their personal data exports.

2.2 *Transferees and purposes*

In analyzing the types of transferees, we found significant differences between the public and private sectors. Public sector organizations, particularly government organizations, transmitted information primarily to other public organizations (80%), a much lower number transmitting data to private firms (the principal exporters here were health and social service organizations). Private firms transfer personal data under their control either to their own multinationals (54%) or to their group or conglomerate (26%). We might say that these were essentially internal flows circulating within these large organizations.

The question of the purposes of the transfers was both sensitive and complex. Our survey revealed that transborder personal data flows were made for a host of purposes, three of which were by far the most significant: personnel management, determination of the eligibility of the individuals concerned for a service, and clientele management. These purposes overlap to some extent. They could be expanded by adding other more specific purposes such as the production of statistics and the marketing and storage of data for possible subsequent use. However, some purposes were more specifically associated with a particular sector. For example, the application of a statute, regulation or public program or criminal legislation is associated with the public sector, while the production of statistics and marketing was the underlying purpose for disclosure by a percentage of private sector respondents that was not negligible.

Finally, we found that none of the purposes set out in our questionnaire was the exclusive domain of respondents in either of the two large sectors. For example, we found public organizations that transferred data for the purpose of trading in information and marketing or producing statistics, just as there are firms that transferred data for the application of a statute or regulation, or criminal legislation.

This overlap in the purposes for which data are disclosed should be examined more thoroughly from the point of view of protecting the rights of the data subjects, particularly when public organizations state that they transfer personal information abroad for purposes relating to marketing or trading in data.

2.3 *Volume and frequency*

With respect to the types of persons who were the subjects of transborder data transfers: a very large majority of public sector respondents (more than three quarters) disclosed information about the people under their administration, a lesser proportion of organizations also disclosing data about their employees. More firms in the private sector disclosed information about their employees than about their clientele. Overall, the proportion of firms or organizations that transferred data about "other" persons was relatively low. There were few apparent differences with respect to frequency of transfers; however, it was noted that in the private sector a large proportion of data transfers concerning employees (48%) occurred more than once a year, while only 25% of transfers concerning customers of firms took place with the same frequency. In the public sector, fewer than one quarter of transfers took place more than once a year, regardless of whether the data concerned employees or persons under the administration of the institution.

In the private sector, disclosures of information dealing with clients generated the largest volumes of transfers. In those subsectors where we found the largest proportion of exporting firms we also found the largest volumes of data transfers. Insurers reported the largest volumes, followed by transportation and tourism firms, financial institutions and associations. In the public sector, where a majority of the respondents disclosed information concerning the people under their administration, only exceptionally was the volume other than small. With respect to employees, the volume was generally not large. With respect to other persons, this volume was even smaller, with a few exceptions such as the direct marketing firm that reported disclosing information with respect to 500,000 "others" during the last year.

We paid particular attention to the questionnaires of the 26 respondents who told us that they transferred very high volumes of personal data (information on at least 10,000 people living in Canada during the last five years). First, we found that a large majority of these respondents were in the private sector, where they accounted for a significant proportion of personal data exporters (13%) compared to the public sector, where the proportion of such exporters was barely 2%. Insurers alone accounted for more than half of the private sector respondents who transferred very high volumes. Generally, personal data transfers were effected mainly by very large organizations and firms and related to the customers of a private firm or the people under the administration of a public institution. However, large volumes of data on people who were neither customers nor employees were transferred by small firms that trade in information.

2.4 *Nature of the data transferred*

With respect to the nature of the data, respondents listed an average of 10 types of information that they transfer abroad. First were the traditional main identifiers: family and given names, date of birth, sex, address and, to a lesser extent, telephone number, marital status and spouse's name. In second place were certain numbers issued by the government for administrative purposes. The social insurance number was most frequently disclosed, especially in the private sector, where a majority of respondents transferred data about their employees, the health insurance number being disclosed principally by health organizations, insurers and tourism firms.

A significant proportion of respondents disclosed data on people's employment status, experience and education, particularly in the private sector where a large majority of respondents transferred data about their employees. Few respondents disclosed data about people's financial status. This may be explained by the small number of firms in the financial sector that responded to our questionnaire. The highest proportion of respondents transferring information about the health of individuals was found in the public sector and among insurers. Physical characteristics such as fingerprints and blood group, and criminal records, were most often transferred by public organizations. Finally, only a very small minority of respondents in both sectors transmitted certain types of highly sensitive data such as religious and political affiliation and other memberships, activities and opinions.

These results permit us to designate certain core groups where either large quantities of personal data or personal data that may be considered "sensitive", depending on the use made of them, are disclosed. However, this does not necessarily assist us in understanding how certain organizations or firms might justify disclosing data that at first glance seem to have little relationship with their main areas of activity.

2.5 *Method and form of disclosure*

A majority of our respondents disclosed select data on an individual more often than complete individual files, sets of data dealing with larger groups of people or complete files covering all available data on all individuals. This primary method of disclosure was used more broadly in the public sector (87.2% of respondents) than in the private sector (64.8%). In the public sector, the results varied little from one group to another while in the private sector professional service firms used this method most often (78.6%). Disclosure of a set of data taken from a group of files was in second place, being most common for tourism or transportation firms and associations. The other two methods of disclosure were used by a very small number of respondents. Transfers of complete files on individuals were effected mostly by transportation and tourism firms and by organizations in the government group, while transfers of complete files covering all data on all individuals were made primarily by insurance firms.

Hard copy records were still the primary form of disclosure used by all firms and organizations that participated in our survey. A minority of public sector respondents used media involving new technologies. The fact that a majority of transfers from this sector related to one individual at a time and that the information was disclosed to multiple transferees certainly explains in part why the traditional forms of disclosure are still widely used. For the private sector, although a much larger proportion of respondents used magnetic media and telematics to send data abroad, this is not to say that they have abandoned the traditional methods of disclosure with the exception, however, of firms in the fields of finance and insurance.

2.6 *Protections and guarantees*

According to our respondents, in a majority of cases the data transferred were well protected and the data subjects were rarely kept unaware of the disclosures. Some results were surprising, so positive a picture did they give of the situation primarily with respect to the protection offered in the private sector. The only case in which public sector respondents offered more protection than the private sector was with respect to informing people concerned by the disclosures of information (80%). With respect to the right of access abroad to data transferred and the right to make corrections, the highest proportion of positive responses was received from the private sector. This result seems abnormally high, more respondents stating that there was an opportunity to make corrections than stated that there was an opportunity to have access to the data transferred.

The responses concerning guarantees offered by transferees indicated great concern on the part of a significant proportion of public sector organizations, and even more among private firms. This was true particularly with respect to the confidentiality of the data. These results are surprising, particularly given that legislation to ensure protection of personal data and access by individuals to data concerning them essentially covers the public sector. Apart from confidentiality, these guarantees relate, in descending order, first to the use of the data and the relevance of the data to the proposed use, and then to security and the length of time data are stored, the responses placing the insurers group well in the lead with the public sector really bringing up the rear.

2.7 *Countries of destination*

With respect to countries of destination, our respondents stated that personal data were transferred to more than 100 countries on all five continents. However, the primary destination for personal data flows was the United States (17% of respondents), particularly in the private sector (20% of respondents). If we use as our reference point the fact that at least 1% of our respondents stated that they transferred personal data abroad, the only countries to which significant transfers of personal data took place were the United States, the United Kingdom, France, the Federal Republic of Germany, Japan, Australia, Hong Kong and Italy. The United States was still the most significant destination, based on an analysis of very large volumes of personal data, this being a particularly important phenomenon in the private sector, especially in the field of insurance. The data that we gathered also allowed us to observe that the private sector transmitted fewer personal data to the European countries than did the public sector, but relatively more to the Pacific region countries.

2.8 *Legal protection abroad*

Personal data originating in Canada enjoy varied forms of legal protection, depending on the legislation in the countries to which they are transferred. Some countries have broad, general legislation protecting personal data that covers both the public and private sectors. This is essentially the case in the Western European countries, primarily the United Kingdom, France and the Federal Republic of Germany. Other countries do not have general legislation but, rather, several pieces of specific legislation protecting personal data and privacy, covering primarily the public sector. This is essentially the case in the United States, Australia and Japan. Finally, there are other countries where there is no general legislation protecting personal data although, on the other hand, there may be certain specific provisions covering activities in certain subsectors of the public or private sectors.

The scope of the legal protection offered varies from country to country. For example, in the United Kingdom, personal data transfers in paper form are not covered by the statute. In Massachusetts, a major destination for personal data in the insurance field, there is no specific legislation to protect insurance records; moreover, there is at present no protection for personal data transferred to private firms in Japan or Hong Kong.

3 Summary of conclusions by groups of sectors

Up to now, our conclusions have dealt with the results considered by theme, for all respondents, for each of the two broad sectors and by groups of subsectors. We will now review the situation within each group of subsectors to provide a complete picture of current practices in each case and to determine the variables that are likely to have an influence on whether personal data are exported. We will present our conclusions by examining the results first for groups in the public sector, and then for those in the private sector.

3.1 Education

This group, which includes school boards, colleges and universities, both public and private, is the second largest group because it accounts for more than one third of all respondents in the public sector who transfer data outside Canada.

Although a large majority of the educational institutions that responded to the survey are small in terms of clientele, this variable does not seem to have any influence at all on whether organizations in this group exported personal data. The number of people they employ seemed to have barely more influence in this respect.

This is the group in which we find the highest proportion of public sector respondents who disclose data about their employees; however, in a majority of cases only a small number of people were affected.

It is therefore not surprising to observe that this group also contains the highest proportion of organizations that disclose information for personnel management purposes, a portion of these transfers perhaps relating to cooperative and international exchange programs. It is also in this group that we find the largest number of organizations that transfer data to "part of their international organization". More surprising, however, is the fact that four respondents disclosed personal data to a firm that traded in information and that an even larger number stated that they did so for purposes of marketing or trading in information. Are these private or public schools? We have nothing to indicate this.

This group contains the highest proportion of organizations that disclose sets of data taken from groups of files, some providing access to or transferring personal data using telematics.

The subjects of the data disclosed by organizations in this sector were, proportionate to other sectors, most likely to be informed of such transfers, to have access to the data transferred and to be able to make corrections. This probably may be explained largely by the fact that the data were very often transferred at the request of the person concerned. In the specific context of education, this fact also probably helps to explain why only a minority of organizations stated that guarantees were always obtained from the transferees, even to ensure that the confidentiality of the data is respected.

Respondents in this group transferred personal data in a significant manner to the United States, the United Kingdom, France, the Federal Republic of Germany and Japan. When data were transferred to other public organizations, they were covered by the provisions in effect in these countries ensuring the confidentiality of the data.

3.2 *Municipal*

More than half of the municipalities and organizations associated with the municipal sector that we contacted responded to our survey. However, given the low proportion of respondents who stated that they exported personal data, these organizations accounted for less than 5% of the exporters in the public sector as a whole.

A majority of municipalities, whether or not they export data, served a population of average size and had fewer than 1,000 employees. Neither the number of clients nor the number of people employed had any influence on the export of personal data by these organizations. For example, only one of the 12 municipalities with more than 1,000 employees exported personal data.

It is in this group of organizations that we found the lowest proportion of respondents who disclosed data about more than one category of people. Paradoxically, a very high percentage of these exporters transferred data about people other than the people under their administration or their employees. There is no indication of the status or number of people affected by these data exports.

With respect to the purposes of the data transfers, the only specific observation that can be made is that two organizations disclosed personal data for marketing purposes.

Four organizations transferred personal data using telematics, only one organization doing so by a method other than disclosure of selected data on an individual.

It is in this group that we found the highest proportion of organizations that transferred data abroad without obtaining guarantees from the recipients, except insofar as concerns the relevance of the information disclosed. Moreover, these organizations also stated that the data subjects were not informed of such disclosures.

3.3 *Health and social services*

Even with the lowest rate of response in the entire public sector, this group was the largest, representing 41% of all exporting organizations. The health subsector, composed primarily of hospitals and medical centres, dominated this group, these same organizations being responsible for the largest share of data exports by this group. It is in this public sector group that both the number of people under the administration of the organizations and the number of people they employ had the greatest impact on whether or not personal data were exported. In fact, we observed that the percentage of exporters rose in direct proportion to the numbers of employees and clients.

A very large majority of the organizations in this group exported data on the people under their administration, outstripping all other groups in the public sector in this respect. In most cases, these transfers concerned a small number of people; only one hospital reported disclosing information with respect to a very large number of people during the last year.

A majority of respondents in this group transferred personal data to distinct firms or persons and did so for purposes of clientele management or the determination of the eligibility of a person for a service, it being possible that these two purposes were concurrent depending on the point of view from which we consider them. Only one organization disclosed data to a firm trading in information, which in this case might have been the Medical Information Bureau.

The proportion of organizations in this group that transmitted "all information available on all persons on file" or a "set of data taken from groups of files" was comparable to the public sector as a whole; however, it was still a large number of organizations (16). It would be useful to examine these data more thoroughly to determine the impact on privacy protection.

Almost all organizations in this sector stated that the people affected by the data they transferred abroad were informed of such disclosures. However, a smaller proportion than in all other public sector groups provided rights of access and correction. We must therefore question the fact that a small majority of organizations stated that the transferees "always" or "in certain cases" provided guarantees concerning the use to be made of the data, the relevance of the data for such use and confidentiality, when a very large majority were not in a position to state that they obtained guarantees as to the security of data and the time for which they would be stored. Given that a majority of organizations disclosed information that was as sensitive as medical records, this question merits more thorough consideration.

With respect to countries of destination, significant numbers of personal data transfers in this sector were made only to the United States and the United Kingdom. Data that were not transferred to public organizations in the United States would not be covered by any legislative protection in that country.

3.4 *Governments*

In this group, composed primarily of departments and organizations not falling into the three other public sector groups, we found the highest rate of participation in the survey and the highest percentage of exporters. Nonetheless, in terms of the percentage of positive responses, it ranked second in the public sector.

A very large majority of organizations in this group that export data had more than 100,000 people under their administration, a minority of such organizations that do not export data also serving such a large clientele. The number of people employed is of less significance in explaining whether or not data were exported than was the number of clients.

Although a large proportion of exporters in this group operated under provincial jurisdiction, the highest proportion of organizations under federal jurisdiction in the study was found here. Moreover, the proportion of exports was nearly twice as high for organizations as for departments. This situation may be explained in part by the division of powers in the Canadian Constitution, a number of federal organizations and departments operating on an international scale.

This is where we found the highest proportion of organizations that export personal data about more than one category of people and about the people under their administration. We also found here a very large percentage of exporters of data about persons "other" than those under their administration or employed by them. This group also led concerning data transfers covering very large numbers of people.

Almost all of these organizations disclosed personal data to a distinct public organization. A very large majority of transfers took place for the purpose of applying a statute, a regulation, a program or criminal legislation. Moreover, a majority of organizations disclosed data to determine a person's eligibility, a purpose that could very well overlap with the previous purposes. Finally, we would note that three organizations stated they disclosed information for the purpose of trading in information.

The proportion of organizations in this group that used all forms of disclosure listed in our survey was higher than the average for the public sector. However, these organizations dominate particularly in the use of telematics: three organizations providing access and 11 others transferring personal data in their possession in this form. There might be a relationship between these practices and the fact that a large proportion of organizations transferred "all information available concerning all persons on file" or "all information available on an individual".

A large proportion of government organizations stated that the subjects of the information they disclose were informed of such transfers only in certain cases or were not informed at all. With respect to guarantees given by the transferees, although this group ranked first in the public sector for proportion of positive responses, a majority stated that only with respect to the confidentiality of data did they always obtain such guarantees.

Government departments and other public organizations transferred personal data in significant occurrences to the United States, France, the FRG and Japan. The transferees in such cases being public organizations, the information disclosed was protected by the general personal data protection legislation that each of these countries has adopted. Data disclosed by departments and organizations that transferred large volumes of personal information were distributed to a host of countries, including the United States, the Caribbean countries and the Western European countries.

3.5 *Associations*

This group included various types of nonprofit associations: professional bodies, religious congregations or organizations, unions and associations of firms, or organizations offering various kinds of services. Associations accounted for a large proportion of all private sector data exporters. They had a much higher rate of positive responses than the private sector average as a whole and, in this respect, were the third-ranking group.

The numbers of clients and employees were important factors in explaining involvement in transborder data flows: there were proportionately more exporters among associations that served very large numbers of clients and among those that employed very large numbers of people.

The numbers of associations that exported personal data about their clients was similar to those that exported data about their employees. One association, a union that identifies its members as "clients", exported personal data concerning a very large number of people.

Proportionately more respondents in this group than in the private sector as a whole transferred data for the purpose of producing statistics. This group also contained a high percentage of associations that transferred data to a public organization and that stated they did so to apply a statute or program.

Almost all associations used traditional forms of disclosure — for example, hard copy records or telephone — to transmit their data, only two associations using telematics. However, being confined to traditional means did not prevent several associations from communicating "all information available concerning all persons on file" or "sets of data taken from groups of files".

A very large majority of associations stated that the subjects of the information disclosed were informed, but a much lower proportion provided rights of access and correction.

Because of the large number of associations that transferred personal data abroad, it was hardly surprising that some destinations could be considered to receive significant volumes. These were the United States, specifically New York, California and Washington states, Japan, France, the FRG and Singapore. Of these destinations, only the European countries, where both public and private sector activities are covered, provided legal protection for personal data about individuals living in Canada.

3.6 *Insurance*

The population in this group was composed of insurance agents and, for the most part, insurers. The highest response rate in the entire private sector was from insurers, who were essentially responsible for transborder personal data flows since only one insurance agent reported such exports. This group of respondents accounted for 15.4% of private sector exporters, ranking third out of the nine groups.

While we found a higher proportion of exporters among insurers serving a clientele of more than 100,000 people, the number of clients offered some, but not a very strong, explanation for the existence of transborder data flows because a very large majority of respondents served a large or very large clientele. In this respect, the number of people employed seems to have had a more significant effect.

Insurers ranked eighth in terms of the proportion of respondents who disclosed information about their employees. It is interesting to note that the same percentage of insurers stated that personal data about their employees were disclosed for personnel management purposes as were transmitted to part of their multinational.

The highest proportion of respondents who exported personal data about their clients was found among insurers. All insurers that exported such data did so with respect to a very large number of people.

A very large proportion of insurers also disclosed personal data in order to determine eligibility for a service, for clientele management or for the production of statistics. Insurers accounted for a very large majority of private sector respondents who transmitted information to a firm that was engaged in trading in information or storing information for later use. While insurers disclosed data to a small number of transferees, this did not mean that there was not a variety of purposes for these disclosures.

Based on the responses provided by insurers, we can say that a close correlation cannot be determined between the use of automated forms of disclosure and the fact that more data sets, or all data about all individuals, were disclosed. In fact, insurers who very seldom used traditional means to disclose data, preferring telematics, disclosed all data or sets of data in only slightly higher proportions than for all private sector respondents. On the other hand, the use of telematics permitted them to disclose information on a very large number of individuals, even if they disclosed only certain data about one individual at a time.

According to a very large majority of insurers, the people affected by the data they transferred abroad were informed of such disclosures and had the greatest opportunity to make corrections. This group is where we found the highest proportion of firms that were able to state that the transferees undertook to provide the five types of guarantees required to ensure protection of privacy. In this respect, we would note only that the data sent to the Medical Information Bureau were surrounded by such guarantees and that the people affected by such disclosures enjoyed three types of protection (information, access, correction).

Eleven insurers stated that they disclosed very large volumes of personal data. They transferred all these data to the United States, either to the state where the parent company of their multinational firm was located or to Massachusetts, where the Medical Information Bureau is located.

We cannot conclude without noting that the participation of insurers in our survey was invaluable for both the precision and the coherence of the responses given. The frankness with which these responses were made was very useful. The quality of their participation indeed testifies to a knowledge of current practices in these firms and demonstrates a particular capacity to appreciate all aspects of the concept of transborder data flows and to control and manage such flows.

3.7 *Business and industry*

This group of firms ranked fifth in the private sector, in terms both of participation and of positive responses. Nevertheless, it was the largest group of exporters in the private sector. It is composed of wholesale and retail businesses, construction firms and primary and manufacturing industries. None of the construction firms contacted exported personal data and only a small proportion of wholesale/retail businesses did so. On the other hand, the highest percentages of exports were found in the primary sector and among manufacturing industries.

For this group, neither the number of clients nor the number of people employed seemed to be a factor in explaining whether or not there were transborder data flows. Although the firms making up this group mainly served small numbers of clients, they employed large numbers of people, whether or not they exported personal data. These results were hardly surprising because, on the one hand, the primary activity of these firms generally did not involve serving the public directly and, on the other, we selected the 500 largest Canadian employers in these sectors of activity.

Almost all respondents in this group exported data about their employees, while, at the same time, ranking last in the private sector in terms of exports of personal data about their clients. It was not, therefore, surprising to note that a very large proportion of firms communicated such data for personnel management purposes and that almost all transferred data to part of their multinational or conglomerate.

No firm that disclosed data about its employees did so with respect to a very large number of people. On the other hand, one retail business was responsible for disclosures of personal data about a very large number of clients. One fact should be mentioned concerning the form of disclosure: respondents in this group disclosed data in automated form less frequently than was the case for the private sector as a whole.

Proportionately fewer firms in this group stated that the data subjects were informed of disclosures, which leads us to wonder, because it was essentially employees who were affected by these disclosures. On the other hand, there is greater opportunity to exercise rights of access and correction here than in any other private sector group. With respect to countries of destination, the respondents in this group transferred personal data mainly to the United States and the United Kingdom.

3.8 *Communications*

Although communications firms ranked second in terms of participation in our survey, they were second-last in terms of the proportion of respondents who exported personal data. The highest proportion of exporters was found among publishers and printers, with very few communications firms, properly speaking, exporting data.

In this group, the number of clients was a very influential variable. A majority of nonexporting firms served very small numbers of clients, while a significant proportion of exporters had very large numbers of clients. The number of people employed was also quite an important variable in explaining the results, since large employers were very heavily represented among exporters.

In this group, which had only 10 personal data exporters, the data transferred related primarily to employees and concerned only a small number of people. The proportion of respondents who exported information about "other" people was higher than the average. However, the number was still very small in terms of occurrences: two respondents, who did not specify the number of people involved in such disclosures.

We would note, however, that one of the two firms that disclosed data about their clients did so with respect to a very large number of people: a cable television firm, which disclosed these data to an American firm to establish its billings.

The number of transferees involved in these data transfers was small, but the number of purposes identified was much larger, except for marketing and purposes that are more closely associated with the public sector.

At first glance, it is paradoxical to state that communications firms had the lowest proportion of respondents who used telematics to transfer data abroad. This may be explained, however, when we recall that a majority of our respondents were in the field of publishing. This may explain why a majority of respondents were not able to respond to the questions about the protections enjoyed by the individuals who were the subjects of the data they disclosed, and the guarantees provided to them by transferees in terms of respecting these rights. The only country to which respondents in this group made significant transfers of personal data was the United States.

3.9 *Financial services*

The financial sector ranked ninth in terms of the response rate to the survey and seventh in terms of the proportion of respondents who exported personal data. Response rates varied considerably from one subsector to another. Banks and deposit institutions dominated, followed by respondents classified under the heading "undetermined finance", which includes composite firms that were difficult to assign to specific subsectors of our population. Well-defined subsectors for which we had a very low rate of response included credit bureaus and credit institutions specifically.

A lower proportion of these firms also engaged in transborder data flows than the average in the private sector. As for the rate of response, we found significant variations among the various subsectors. On the one hand, the subsectors composed of banks and deposit institutions and real estate agents had a higher proportion of exporters; on the other, major subsectors such as trusts, real estate, securities brokers and credit institutions had no exporting firms. This does not seem to reflect a realistic picture of the situation.

The number of clients seems to exert some influence on whether or not there are transborder personal data flows. However, the number of employees is not an influential variable, with equal numbers of exporting and nonexporting firms in the various categories of employers.

This is the group in which we found the lowest proportion of respondents who disclosed information about more than one category of people. In a majority of cases, these disclosures related to clients. However, a few respondents disclosed information about their employees. These results may be explained in part by the fact that several subsectors did not respond to our questionnaire. We have good reason to believe that we would have found subsidiaries, or members of multinationals, among these firms that exported data about both clients and employees, not to mention credit bureaus that disclosed information about "other" people. However, a majority of these firms declined to participate in our survey. Among the rare firms who provided a figure for the number of individuals affected by disclosures of information, two transferred data about a very large number of people: one credit bureau that disclosed information about "other" people, and one undetermined firm that disclosed information about its clients.

This is the group in which we found the lowest proportion of firms that export personal data to part of their multinational or to a firm in the same group. On the other hand, a higher proportion transferred such data to a distinct firm or to a firm engaged in trading in information, and did so for purposes of marketing or trading in information. Moreover, a very significant proportion of respondents used telematics to transfer or provide access to data in their possession, with a corresponding lower use of the traditional forms of disclosure. We cannot find, however, any particular impact of this fact on the communication methods in this field.

A very large majority of respondents informed the data subjects that the data were being disclosed and provided the right to access such information and to make corrections. In this sector of activity, we also found one of the highest proportions of respondents who stated that they obtained guarantees from recipients as to the use that would be made of the information, the relevance of the data transferred to the declared uses and the time for which the data would be stored.

Overall, the respondents in this group stated that they transferred personal data mainly to the United States. However, the two respondents who transferred very large volumes of personal data did so to more than 20 countries. In the United States, there is a host of legislation to regulate in one way or another the operations involving data about an individual's financial status.

We cannot close without mentioning the fact that the firms in this sector of economic activity that participated in our survey were not all in a position to respond to specific questions. A high percentage of respondents were not, in fact, able to provide a figure for the number of clients about whom personal data were disclosed or to identify the transferees and purposes of such disclosures. That leads us to conclude that we would have to use another approach in order to obtain a more realistic and complete picture of the situation that prevails in this sector in the area of transborder personal data flows.

3.10 Transportation and tourism

Only a small percentage of firms in this group responded to our questionnaire, a tiny minority of respondents stating they exported personal data. Thus this group ranked last among the private sector groups even though we would have expected a greater level of international activity in the area of data transfers, particularly on the part of air carriers. However, the finer points of these results should be noted in order to account for significant contrasts. First, a large proportion of transportation firms and air carriers responded to our questionnaire, thus ranking second and third for rate of response immediately behind insurers. However, only a tiny minority of air carriers told us they exported personal data. On the other hand, a large proportion of travel agents exported personal data.

The number of clients was of considerable value in explaining whether or not there were transborder data flows. While the number of employees was of some explanatory value, it had much less influence than the clientele variable.

Although there were few respondents in this group (10), they were major exporters of personal data. First, they disclosed information about their clients, their employees or more than one category of people in higher proportions in all cases than the average for the private sector. Some firms disclosed personal data about a very large number of people, this group ranking second behind insurers. In three cases, these were tourism firms transferring data about their clients and the fourth was a transportation firm transferring data about its employees to part of its multinational firm.

There was a correlation between the number of respondents who stated that they disclose data about their clients and those who did so to determine eligibility for a service. The firms in this group on average identified the largest number of transferees per respondent; the only transferee not indicated was telecommunications firms. Despite this diversity, intra-company flows were effected by a very large proportion of firms in this group.

This sector of activity was unusual in relation to the private sector as a whole in terms of the methods and forms of disclosure. Only a minority of respondents disclosed select data concerning an individual, with correspondingly higher rates for the other methods of disclosure. This group also had the highest proportion of firms that used magnetic media to transmit data and provided access by telematics to information in their possession without, however, abandoning the traditional forms of disclosure.

When we analyze the destinations of personal data transferred by respondents in this group, only the United States warrants particular attention. Not only did a significant proportion of respondents tell us that they exported data of this nature: four of them stated that they transferred large volumes of personal data to one or more American states. No specific protection was given to personal data held by firms in this sector under American law.

3.11 Computer services

The firms in this group ranked second in the private sector in terms of the percentage of respondents who transferred personal data abroad. The number of clients had no impact on whether or not there were transborder data flows. On the other hand, the number of employees played a major role in this respect. While there were equal numbers of exporters in the four categories of employers, a majority of the nonexporting firms consisted of small employers, this proportion falling constantly as the number of employees rose.

This group had the highest percentage of respondents who disclosed data about more than one category of people. The firms in this sector ranked second among private sector groups in terms of the proportion of respondents who transferred data about their employees, but only two of them did so with respect to a large number of people.

It is surprising to find that a very large majority of the firms in this group transferred only select data, with a corresponding decrease in use of other methods of disclosure. With respect to the form of disclosure used, we would note only that a large proportion of firms uses magnetic media rather than hard copy records.

It was current practice for a significant proportion of respondents in this group to inform people of the disclosure of personal data concerning them and to obtain guarantees from transferees as to the security of the information and the time it would be stored. The United States is the only significant destination identified by respondents in this group.

3.12 Professional services

Professionals ranked third in the private sector in terms of the rate of participation in our survey, surpassing all other groups in terms of the rate of positive responses. On this point, accounting firms took first place. The number of clients variable was not a factor in explaining whether or not there were transborder data flows. On the other hand, the number of employees is a major factor in explaining exports of personal data, nearly half of the exporters being very large employers. In this respect, this group ranked first in the private sector.

With respect to the categories of people affected by personal data exports, the results for this group are in all respects comparable to those for the private sector as a whole: a higher percentage of respondents transferred data about their employees than about their clients, and more than a quarter of respondents transferred data about more than one category of people. In every case, a small or average number of people were affected by such transfers.

We would note only that a higher-than-average proportion of respondents disclose personal data in order to apply a statute, program or regulation, and that a higher percentage of respondents sent such information to a public organization abroad. Professionals ranked second in terms of the average number of transferees identified per respondent.

A very large majority of firms disclosed certain data about an individual, using various means of disclosure in the same proportion as private sector firms as a whole.

According to a very large majority of respondents, the people affected by the disclosure of personal data were informed of this fact, had access to the information transferred and could make corrections to it. However, only a minority of firms was in a position to state that transferees assured them that they would comply with the various types of guarantees listed in our questionnaire.

Respondents in this group were exceptional in the fact that they transferred significant volumes of personal data to several countries. The United States was in first place among the countries of destination, all exporters transferring personal data to that country. Personal data were also transferred to the United Kingdom, France, Japan, the FRG and Australia.

3.13 Miscellaneous services

Only a minority of firms in this group responded to the questionnaire, and only a quarter of these exported personal data. We therefore found ourselves with 10 exporters divided into five subsectors of activity, making any statistical analysis of the results by subsector impossible. Some general observations should, however, be made. First, we should mention that a very low percentage of security firms, which represent almost half of the population for this group, participated in the survey and only one of these respondents stated that it exported personal data. Only in the employment and advertising subsectors did we find more than one exporter. As these subsections accounted for a very large majority of the respondents in this group, we were able to assert the importance of transborder flows of personal data relating to employment and advertising.

A majority of the firms in this sector served small numbers of clients, a factor that might be of some slight assistance in explaining whether or not there are transborder data flows. The number of employees in no way contributes to explaining this phenomenon. We would note only that while a very large majority of respondents was composed of small or medium-sized employers, these appeared in greater proportion as exporters of personal data, a situation almost unique in relation to what we have observed in the private sector as a whole.

This group had the highest proportion of respondents who disclosed information about people other than clients or employees. It had only four firms. One of the respondents disclosed such information about a very large number of people. It was a direct marketing firm that disclosed data normally found on mailing lists to various firms.

It is surprising to find that, despite the heterogeneity of the firms that make up this group, nearly all respondents sent information to part of their multinational or to a firm belonging to the same group as they do. A much higher proportion of service firms than the average in the private sector disclosed all information held on an individual, while using telematics to transfer this data proportionately less often.

We would note only that the marketing firm that told us it transferred a high volume of data abroad reported that the people affected by these transfers were not informed of this fact and, accordingly, they did not have access to and could not correct the data thus transferred. Finally, the transferees of this information offered no guarantee as to the use to be made of it or the protection given its confidentiality.

A significant number of respondents in this group stated they transferred personal data to the United States, specifically to New York

State, and to France. We would also note that the only marketing firm reporting the export of personal data indicated that, during the last year, it transferred personal data dealing with 500,000 people to New York State and Illinois.

4 Conclusions from the study and significance of conclusions

To summarize, the general picture that we find from our study is one of moderate exports of personal data about Canadians. Such exports occurred more often in the private sector (where these flows are primarily intra-company) than in the public sector, both in terms of frequency and volume. These exports related to personnel management and client service concerns more often than to selling or exchanging information. They also involved quite varied types of information. These data transfers generally occurred without the use of intermediaries, related only to select data in files, and were effected primarily by telephone or in writing, although electronic methods of data transfer were also used in some sectors. These flows were destined mainly to the United States of America and, secondarily, to the European and Pacific countries.

A majority of our respondents stated they offered reasonably complete protection and guarantees. This was so above all in the private sector, which has no obligation to provide such guarantees (although this was also the case in the public sector, some parts of which must apply privacy legislation to their files). The legal protection applied abroad varies considerably in comparison to the Canadian situation. The European countries require general protection for all information, including information in the private sector, while the United States, Japan and Australia have adopted this sort of protection exclusively for the public sector. However, we should note, in strong contrast to the Canadian situation, that there is a host of legislation in the United States regulating various private sector activities, and that only American citizens enjoy constitutional protections since the very recent interpretation given by the United States Supreme Court in *Verdugo-Urquidez*.

Generally speaking, we believe that this study provides a realistic picture of the situation in the sectors where there was a reasonable rate of precise responses. In this respect, we would note that among the most important responses were those from insurers and industrial firms, which provided us with complete, consistent responses permitting an appropriate assessment of their exports of personal data.

However, our survey leaves a shadow over some very large data flows because of the poor participation by certain categories of firms such as the large banks, credit institutions, credit card issuers and credit bureaus, as well as investment companies, securities brokers and large air carriers. We also believe that the figures for the electronic and telephone communications firms and security services are lower than we might have expected.

The inability of a large number of respondents to provide specific numbers for the large volumes of data they exported affected the study. Some public governmental organizations also have high volumes of exports that were not always easy to state in quantitative terms, given their dispersed nature. Moreover, we did not survey small and medium-sized firms and smaller public organizations, although they might be responsible for large exports of personal data because of the growing availability of technological methods of transferring data and the establishment of increasingly accessible communications networks.

We also believe that technological change will characterize the expansion of new methods of disclosure such as consultation of personal data bases held in Canada from points abroad. The volume and frequency of such activities will be increasingly difficult to assess if we do not have the technical resources to identify them and determine their frequency and content.

If we want to answer the primary question posed by this study, we may state that there are transborder personal data flows in practically all sectors of activity, with great variations in the volumes and the practices followed. In this sense, the problem of protecting exported personal data exists everywhere to varying degrees and remains current in the growing internationalization of economic and information exchanges. The great variety of legislative and contractual protection applied abroad to information about Canadians justifies a serious examination by Canadian authorities of the value of the protection and rights made available to Canadians for their benefit and the appropriateness of controlling data exports to countries that do not offer protection equivalent or comparable to what is provided in Canada. It would be appropriate to examine the advisability of making Canadian protection comparable to the protection offered in countries that attach much more importance to such protection and that might refuse to authorize the export of data about their nationals to Canada if this country does not provide them with guarantees of protection comparable to what is enjoyed at home.

These results make this study one of the most original and best documented in the field of international transfers of personal data and in the study of the legal protection applied to such data. It confirms and complements the results of earlier research studies by our group and by international bodies. It has no equivalent in the literature of the various countries we have studied. It offers a striking portrait of the various parameters that illustrate and explain the development of the phenomenon of personal data exports. It identifies the sectors where we are still lacking information and where there should be more thorough analysis. It integrates analysis of the legal parameters with analysis of the phenomena of personal data exports to determine the impact and significance of the law in the context of international data transfers.

Finally, to broaden our perspective, we cannot close without noting the important issues involved in the question of transborder data flows, both for the trade in data and the development of our computer and telecommunications industries, and for the preservation of Canada's national sovereignty. However, it was not within our mandate to consider these aspects of the question. Let it suffice for us to mention here that studies conducted in the United States have not demonstrated that regulation of personal data protection has created any significant barriers to the free flow of data, and that problems of sovereignty arise more than ever with the recent decision of the United States Supreme Court claiming to make foreigners subject to the laws of that country without providing them in return with the fundamental constitutional guarantees that justify and govern the application of those laws. We would also note a resurgence of interest in the European countries in personal data protection issues, particularly with the approach of economic union in 1992 and the repercussions that this could have on trade with the North American subcontinent and on developments in practices in Canada and the United States in the wake of the Free Trade Agreement.

5 Assessment of the research experience and acknowledgments

It remains for us to set out, in conclusion, our assessment of the research experience, which was in all respects positive. We wanted to meet a challenge: to carry out an extremely broad national survey and an extensive study of hundreds of pieces of legislation in a record six-month time. We had to work at double speed, because of our success in obtaining a rate of response exceeding all expectations, because of the abundance of documentation that we discovered, and because of last-minute changes imposed by an important decision of the highest judicial authority of our weighty neighbour to the south.

We are happy to have succeeded in producing a substantial report, based on the responses that some 1,800 private firms and public organizations that participated in the survey were kind enough to provide to us, as well as the responses of the commissioners and diplomats who provided invaluable information on the state of the legislation in their countries. We further benefited from the critical review and invaluable advice of our colleagues Jean-Pierre Lemasson, director of the Bureau de la coopération internationale of UQAM, and Pierre Mackay, project director, who acted as members of our research team; and from very fruitful discussions with professors Yves Poullet, director of the Centre de recherche informatique et droit of Namur; Herbert Burkert, of the National Research Centre on Information and

Computers (GMD) of Cologne; and Paul Bernard, of the sociology department of the University of Montreal.

We also acknowledge the considerable contributions of Geneviève Moulin-Picard, who did the detailed analysis of the data taken from our 1988 survey; of the GRID documentation centre librarian, Serge Gariépy; and of our students Denis Poitras and Yvan Poulin Salmons. We are grateful for the steady work of the staff of the GRID secretariat, Hélène Lévesque and Jeanne Benoist, and of the secretariat of the Département des sciences juridiques, who were called into strenuous service in receiving questionnaires and telephone calls in the fall of 1989 and in producing our various reports. We also benefited greatly from the comments of Francine Courtemanche, Head of Editorial Services at the federal Department of Justice.

We should also note the attentive and sustained work provided by our sub-contractors, Data Marketing Inc and Promo-Laser Inc, and particularly by Normand Lesage, Christiane Pichette and Pierre Gagné, in sending out the questionnaires and in the statistical processing of the responses. The quality of the presentation they provided to us undoubtedly explains in part the exceptional rate of response we obtained and points out that it is entirely to their credit that they grasped and processed a much larger volume of responses than anticipated.

APPENDIX 1

Questionnaire

**STUDY ON THE FLOW OF PERSONAL DATA
ACROSS CANADIAN BORDERS**

Please do not write here

General Information

1 ☐☐
3 ☐☐

1. a) Please give the principal activity of your firm or public institution:

____ 5 ☐☐

b) To which field do these activities mainly relate? *(Please check √ your answers)* 7 ☐

Private sector:	Associations	__	Insurance	__
	Retail & Wholesale	__	Finance	__
	Transport, tourism	__	Communications	__
	Service to firms		Industry	__
	Other	__		
Public sector:	Education	__	Municipal	__
	Health/Welfare	__	Government Department	__
	Other institution	__		

8 ☐

c) What is your approximate number of clients? 9 ☐

(Please check √ for your whole firm or institution in Canada):

Less than 10 000 -> __ -> 10 000 to 50 000 __
50 000 to 100 000 __ More than 100 000 __

d) What is your approximate number of employees? 10 ☐

(Please check √ for your whole firm or institution in Canada):

Less than 100 __ 100 to 500 __
500 to 1 000 __ More than 1 000 __

e) Under which jurisdiction do your main activities take place?

federal jurisdiction? __ or provincial? __ 11 ☐

May we suggest that you first read all the following questions (2 to 10) to ensure that your answers are fully relevant

Questionnaire (continued)

Personal Information Transfers

Please do not write here

2. In the course of your operations, do you transfer data to a foreign destination, on a regular or occasional basis, concerning persons living in Canada or Canadians living abroad (by sending out such data or giving access to it)? yes ____ no ____ 12☐

If yes, please go to question 3

If no: Do you transfer such personal data to any other Canadian firms or institutions which retransfer them beyond Canadian borders? yes ____ no ____ 13☐

If negative, please send us back the questionnaire for statistical purposes. Thanks for your cooperation!

If yes: Is this firm or institution *(Please check √ your answers):*

a) a telecommunications agency? ___ 14☐☐
b) a distinct business in the information trade? ___
c) a head office or subsidiary? ___
d) a government or public institution? ___
e) other *(specify)*________________________ 16☐

Please answer the following questions as if you yourself were transferring this information abroad.

3. a) Does the personal data transferred to a foreign destination pertain to your employees, your clientele, or other persons?
(Please check √ all possible answers):
Clients ____ Employees ____ Others ____ 17☐

b) Are these personal data transfers carried out on a regular or occasional basis?
regular? _____ occasional? _____ both? _____ 18☐

c) Approximately how many individuals had their data transferred during this last year? *(If impossible to estimate, please answer with a "?")* 19☐
Clients: _________ Employees: _________ Others: _________ 20☐☐

d) Approximately how many individuals had their data transferred during the last five years? *(If impossible to estimate, please answer with a "?")* 22☐
Clients: _________ Employees: _________ Others: _________ 23☐☐

Questionnaire (continued)

Please do not write here

e) What would be the approximate total number of individuals whose personal data is held abroad due to transfers originating from your firm or institution?
(If impossible to estimate, please answer with a "?")
Clients: ________ Employees: ________ Others: ________ 25☐ 26☐☐

f) What is the average approximate number of data transfers per person per year?
(If less than once a year, please write -1)
(If impossible to estimate, please answer with a "?")
Clients: ________ Employees: ________ Others: ________ 28☐ 29☐☐

Destination of personal data

4. To which types of foreign firms or institutions do you transfer your personal data?
(Please check √ all possible answers or give percentage (%) volumes if available):
a) to a foreign part of your firm or international organization ____ 31☐
b) to a firm member of your group, conglomerate, etc. ____ 32☐
c) to a telecommunication agency ____ 33☐
d) to a distinct business in the information trade ____ 34☐
e) to a distinct private firm or individual ____ 35☐
f) to a distinct public institution ____ 36☐

5. For which purposes is personal information being transferred abroad?
(Please check √ all possible answers):
a) Personnel management ____ 37☐
b) Determination of a person's eligibility for a service ____ 38☐
c) Client or membership service operations ____ 39☐
d) Market research ____ 40☐
e) Production of statistics ____ 41☐
f) Sale & exchange of information ____ 42☐
g) Application of penal or criminal provisions ____ 43☐
h) Application of a law, a regulation, or a public program ____ 44☐
i) Storage of information for undetermined later use ____ 45☐
j) Other ends *(Please specify)* ________________________ 46☐

Questionnaire (continued)

6. Please indicate the countries to which the personal data is transferred:
(Please check √ all possible answers)

Please do not[4] write here

___ U.S.A.: 1 State only *(indicate the State:)* ______________ 47☐
___ U.S.A.: 2 to 5 States *(indicate the 3 most important States:)*
______________ 48☐☐
___ U.S.A.: 6 to 10 States *(indicate the 3 most important States:)*
______________ 50☐☐
___ U.S.A.: 11 to 30 States *(indicate the 3 most important States:)*
______________ 52☐☐
___ U.S.A.: 31 to 52 States *(indicate the 3 most important States:)*
____
___ Central American, South American or Carribean countries 54☐☐
(indicate the 3 most important countries:) 56☐☐
______________ 58☐☐
___ Great Britain 60☐
___ France 61☐
___ Federal Republic of Germany *(indicate the most important Land)*
______________ 62☐
___ Other Western European countries *(indicate the 3 most important countries:)* 63☐☐
______________ 65☐☐
67☐☐
___ Eastern European countries *(indicate the 3 most important countries:)* 69☐☐
______________ 71☐☐
73☐☐
___ Japan 75☐
___ Other Asian countries *(indicate the 3 most important countries:)* 76☐☐
______________ 78☐☐
80☐☐
___ African countries *(indicate the 2 most important countries:)* 82☐☐
______________ 84☐☐
___ South Pacific countries *(indicate the 2 most important countries:)*
______________ 86☐
___ To more than 20 countries 87☐
___ To more than 50 countries 88☐

Questionnaire (continued)

Nature of personal information transferred

7. Among the following information items, please indicate those which you transfer abroad:
(Please check √ all possible answers)

				Please do not write here 5
a) family name & given name ->	___ ->	b) sex ->	___	89 ☐☐
c) permanent address	___	d) telephone number	___	91 ☐☐
e) birth date	___	f) birth place	___	93 ☐☐
g) citizenship	___	h) ethnic or national origin	___	95 ☐☐
i) photograph	___	j) fingerprints	___	97 ☐☐
k) blood type	___	l) language of communication	___	99 ☐☐
m) social insurance number	___	n) driver's licence number	___	101 ☐☐
o) health insurance number	___	p) other identification number	___	103 ☐☐
q) father's name	___	r) mother's name	___	105 ☐☐
s) marital status	___	t) name of spouse	___	107 ☐☐
u) employment history	___	v) employment information	___	109 ☐☐
w) criminal/penal history	___	x) civil judicial background	___	111 ☐☐
y) financial history	___	z) current financial situation	___	113 ☐☐
aa) credit rating	___	bb) education, diplomas	___	115 ☐☐
cc) medical history	___	dd) results of psychological tests	___	117 ☐☐
ee) state of health	___	ff) social program beneficiary	___	119 ☐☐
gg) political affiliation	___	hh) union membership	___	121 ☐☐
ii) religious affiliation	___	jj) other association membership	___	123 ☐☐
kk) applications by person for a service, job, etc.	___	ll) correspondance of person with institution or firm	___	125 ☐☐
mm) person's opinions	___	nn) opinions of others about person	___	127 ☐☐
oo) other personal information *(Please specify)*		______________________		129 ☐☐

8. In which of the following forms do you usually transfer your personal data?
(Please check √ all possible answers or give percentage (%) volumes if available):

a) Communication of all information held on all individuals	____	131 ☐
b) Communication of a series of information items drawn from a series of individual files	____	132 ☐
c) Communication of all information held on an individual	____	133 ☐
d) Communication of a few items of information drawn from an individual's file	____	134 ☐

Questionnaire (continued)

Please do not write here

Means of communication

9. Which means of communication are generally used for your personal data transfers?

(Please check √ all possible answers or give percentage (%) volumes if available):

a) Magnetic (tapes, discs, etc...) ____ 135☐
b) Telecommunication (access to your data available from abroad) ____ 136☐
c) Telecommunication (transfer by your services) ____ 137☐
c) Manuscript (including fax) ____ 138☐
d) Telephone (verbal) ____ 139☐

Protection and guarantees

10. When you transfer personal data to a foreign destination:

a) Are the affected individuals informed of these communications?

always ____ in certain cases ____ never ____ 140☐

b) Can these individuals: *(if positive, please check √)*

- obtain access abroad to the transferred data? ____ 141☐
- have this data corrected abroad, if there is cause? ____ 142☐

c) Do you receive from your foreign recipients guarantees concerning:

(if positive, please check √ all possibilities):	*always*	*in certain cases*	
- the eventual uses of data transferred?	____	____	143☐
- the relevance of data for such uses?	____	____	144☐
- the confidentiality of data?	____	____	145☐
- the security of data and communications?	____	____	146☐
- the time for which information will be held?	____	____	147☐

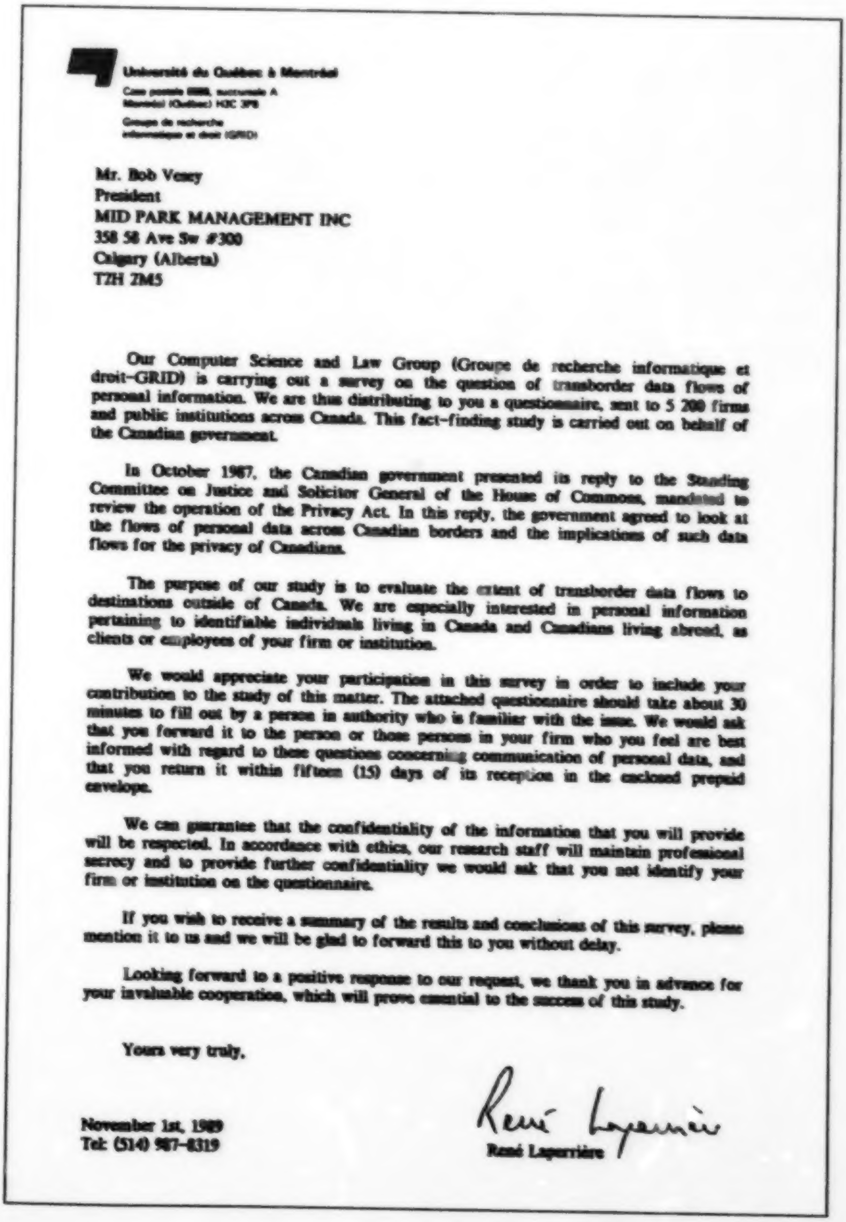
If you have models of instructions, forms, contract clauses or codes of ethics pertaining to the foreign protection accorded to transferred data, and to the law applicable to such transfers, we would be grateful if you could forward them with your questionnaire, or under separate cover.

Many thanks for your cooperation!

Please send your completed questionnaire in the attached pre-paid envelope, addressed to:
Computer Science and Law Research Group (GRID), Suite T-4860,
University of Quebec in Montreal, P.O. Box. 8888, Stn. A, Montreal Qc, H3C 3P8

APPENDIX 2

Letter of introduction



Université du Québec à Montréal
Case postale 8888, succursale A
Montréal (Québec) H3C 3P8
Groupe de recherche
informatique et droit (GRID)

Mr. Bob Vesey
President
MID PARK MANAGEMENT INC
358 58 Ave Sw #300
Calgary (Alberta)
T2H 2M5

Our Computer Science and Law Group (Groupe de recherche informatique et droit-GRID) is carrying out a survey on the question of transborder data flows of personal information. We are thus distributing to you a questionnaire, sent to 5 200 firms and public institutions across Canada. This fact-finding study is carried out on behalf of the Canadian government.

In October 1987, the Canadian government presented its reply to the Standing Committee on Justice and Solicitor General of the House of Commons, mandated to review the operation of the Privacy Act. In this reply, the government agreed to look at the flows of personal data across Canadian borders and the implications of such data flows for the privacy of Canadians.

The purpose of our study is to evaluate the extent of transborder data flows to destinations outside of Canada. We are especially interested in personal information pertaining to identifiable individuals living in Canada and Canadians living abroad, as clients or employees of your firm or institution.

We would appreciate your participation in this survey in order to include your contribution to the study of this matter. The attached questionnaire should take about 30 minutes to fill out by a person in authority who is familiar with the issue. We would ask that you forward it to the person or those persons in your firm who you feel are best informed with regard to these questions concerning communication of personal data, and that you return it within fifteen (15) days of its reception in the enclosed prepaid envelope.

We can guarantee that the confidentiality of the information that you will provide will be respected. In accordance with ethics, our research staff will maintain professional secrecy and to provide further confidentiality we would ask that you not identify your firm or institution on the questionnaire.

If you wish to receive a summary of the results and conclusions of this survey, please mention it to us and we will be glad to forward this to you without delay.

Looking forward to a positive response to our request, we thank you in advance for your invaluable cooperation, which will prove essential to the success of this study.

Yours very truly,

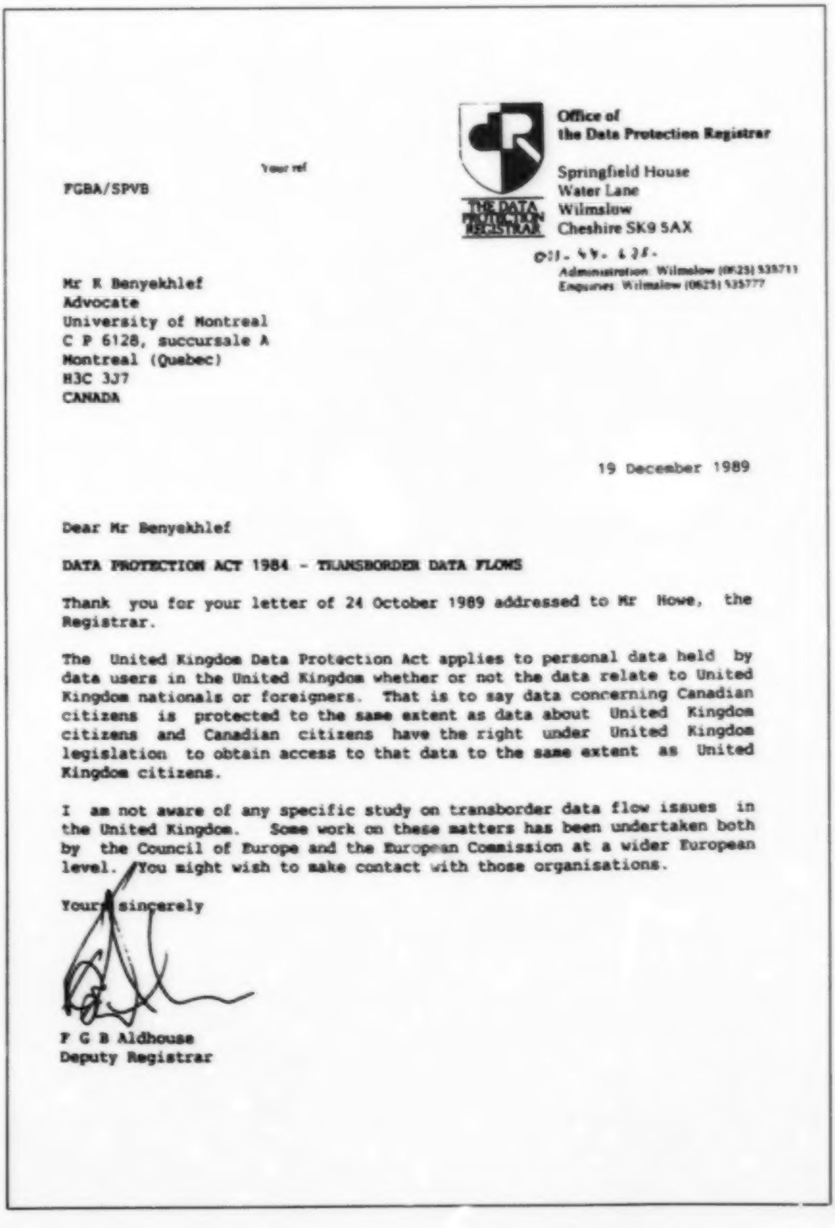
René Laperrière

René Laperrière

November 1st, 1989
Tel: (514) 987-8319

APPENDIX 3

Letter from the Data Protection Registrar of the United Kingdom



THE DATA PROTECTION REGISTRAR

Office of
the Data Protection Registrar

Springfield House
Water Lane
Wilmslow
Cheshire SK9 5AX

011. 44. 625.
Administration Wilmslow (0625) 535711
Enquiries Wilmslow (0625) 535777

Your ref

FGBA/SPVB

Mr K Benyekhlef
Advocate
University of Montreal
C P 6128, succursale A
Montreal (Quebec)
H3C 3J7
CANADA

19 December 1989

Dear Mr Benyekhlef

DATA PROTECTION ACT 1984 - TRANSBORDER DATA FLOWS

Thank you for your letter of 24 October 1989 addressed to Mr Howe, the Registrar.

The United Kingdom Data Protection Act applies to personal data held by data users in the United Kingdom whether or not the data relate to United Kingdom nationals or foreigners. That is to say data concerning Canadian citizens is protected to the same extent as data about United Kingdom citizens and Canadian citizens have the right under United Kingdom legislation to obtain access to that data to the same extent as United Kingdom citizens.

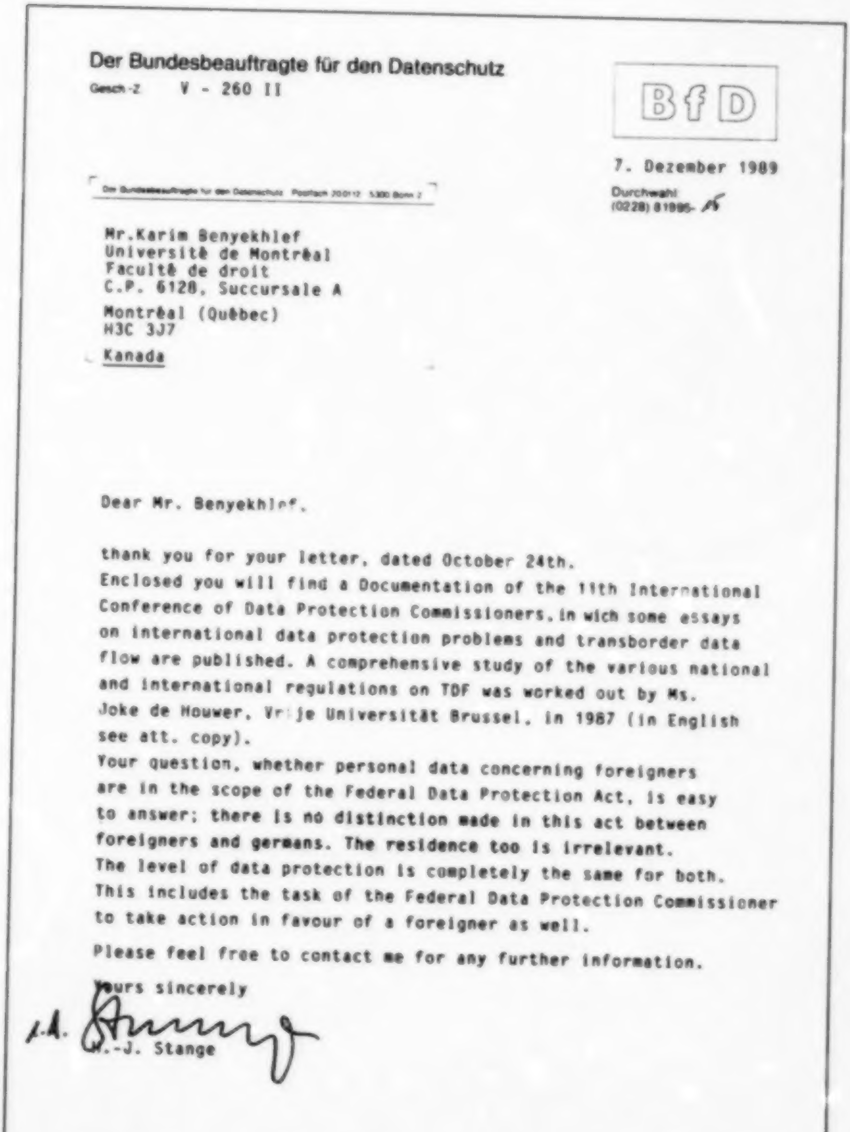
I am not aware of any specific study on transborder data flow issues in the United Kingdom. Some work on these matters has been undertaken both by the Council of Europe and the European Commission at a wider European level. You might wish to make contact with those organisations.

Yours sincerely

F G B Aldhouse
Deputy Registrar

APPENDIX 4

Letter from the Bundesbeauftragte für den Datenschutz of the Federal Republic of Germany



Der Bundesbeauftragte für den Datenschutz
Gesch.-Z. V - 260 II

BfD

7. Dezember 1989

Durchwahl
(0228) 81995-

Der Bundesbeauftragte für den Datenschutz Postfach 20 01 12 5300 Bonn 2

Mr.Karim Benyekhlef
Universitè de Montrèal
Facultè de droit
C.P. 6128, Succursale A
Montrèal (Quèbec)
H3C 3J7
Kanada

Dear Mr. Benyekhlef,

thank you for your letter, dated October 24th.
Enclosed you will find a Documentation of the 11th International Conference of Data Protection Commissioners, in wich some essays on international data protection problems and transborder data flow are published. A comprehensive study of the various national and international regulations on TDF was worked out by Ms. Joke de Houwer, Vrije Universität Brussel, in 1987 (in English see att. copy).
Your question, whether personal data concerning foreigners are in the scope of the Federal Data Protection Act, is easy to answer; there is no distinction made in this act between foreigners and germans. The residence too is irrelevant. The level of data protection is completely the same for both. This includes the task of the Federal Data Protection Commissioner to take action in favour of a foreigner as well.

Please feel free to contact me for any further information.

Yours sincerely

i.A.
H.-J. Stange

APPENDIX 5

Map of occurrences of transfers per country or continent

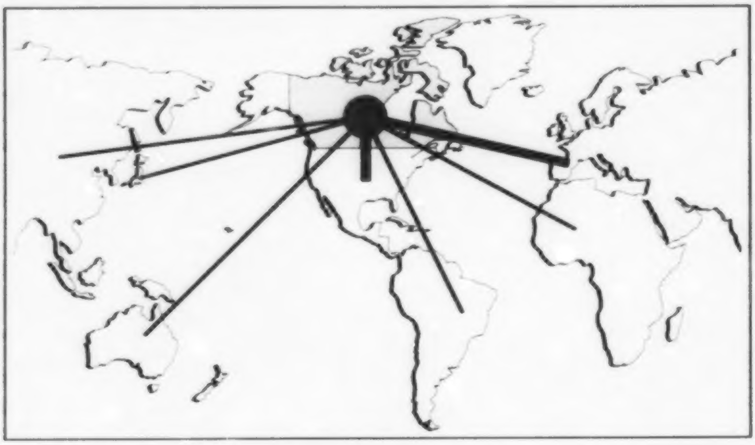
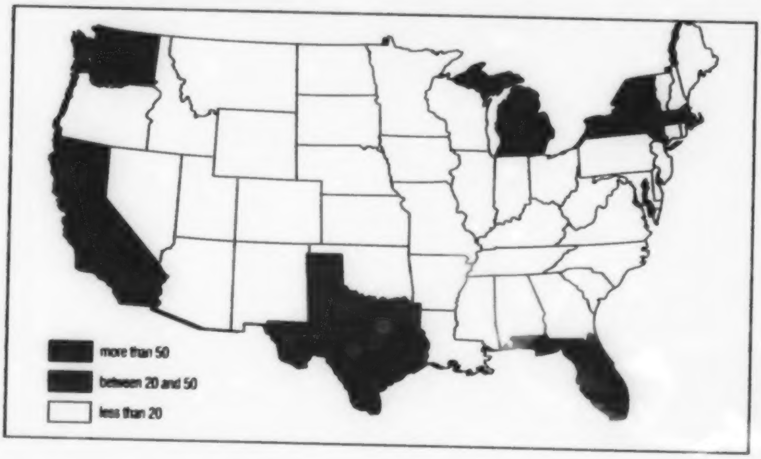


Table 1-2 (from page 214)
Transfers by country or continent

Country/continent	Occurrences	Occurrences /N respondents (%)	Occurrences /N exporters (%)
United States of America	303	17.19	81.23
Great Britain	126	7.15	33.78
France	95	5.39	25.47
Western Europe	69	3.91	18.50
Federal Republic of Germany	65	3.69	17.43
Asia	61	3.46	16.35
America	61	3.46	16.35
Japan	56	3.18	15.01
South Pacific	50	2.84	13.40
Africa	47	2.67	12.60
Eastern Europe	25	1.42	6.70

APPENDIX 6

Map of relative occurrences of transfers to the United States



Extract of Table 1-4 (from page 216) Significant destinations in terms of occurrences (including American states)

states	Occurrences	Occurrences /N of respondents (%)
New York	78	4.42
California	52	2.95
Florida	50	2.84
Washington	30	1.70
Michigan	25	1.42
Massachusetts	23	1.25
Texas	22	1.19